H.R. 4585—THE MEDICAL FINANCIAL PRIVACY PROTECTION ACT

HEARING

BEFORE THE

COMMITTEE ON BANKING AND FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

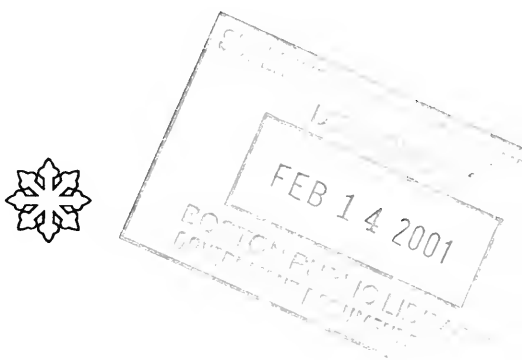
ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JUNE 14, 2000

Printed for the use of the Committee on Banking and Financial Services

Serial No. 106–63



U.S. GOVERNMENT PRINTING OFFICE

65–149 CC WASHINGTON : 2000

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

JAMES A. LEACH, Iowa, *Chairman*
BILL MCCOLLUM, Florida, *Vice Chairman*

MARGE ROUKEMA, New Jersey
DOUG K. BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
RICK LAZIO, New York
SPENCER BACHUS III, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
TOM CAMPBELL, California
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
JACK METCALF, Washington
ROBERT W. NEY, Ohio
BOB BARR, Georgia
SUE W. KELLY, New York
RON PAUL, Texas
DAVE WELDON, Florida
JIM RYUN, Kansas
MERRILL COOK, Utah
BOB RILEY, Alabama
RICK HILL, Montana
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES JR., North Carolina
PAUL RYAN, Wisconsin
DOUG OSE, California
JOHN E. SWEENEY, New York
JUDY BIGGERT, Illinois
LEE TERRY, Nebraska
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania

JOHN J. LAFALCE, New York
BRUCE F. VENTO, Minnesota
BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
KENNETH E. BENTSEN JR., Texas
JAMES H. MALONEY, Connecticut
DARLENE HOOLEY, Oregon
JULIA M. CARSON, Indiana
ROBERT A. WEYGAND, Rhode Island
BRAD SHERMAN, California
MAX SANDLIN, Texas
GREGORY W. MEEKS, New York
BARBARA LEE, California
FRANK R. MASCARA, Pennsylvania
JAY INSLEE, Washington
JANICE D. SCHAKOWSKY, Illinois
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
STEPHANIE TUBBS JONES, Ohio
MICHAEL E. CAPUANO, Massachusetts
MICHAEL P. FORBES, New York

BERNARD SANDERS, Vermont

CONTENTS

WITNESSES

WEDNESDAY, JUNE 14, 2000

Page

APPENDIX

Additional Material Submitted for the Record

H.R. 4585—THE MEDICAL FINANCIAL PRIVACY PROTECTION ACT

WEDNESDAY, JUNE 14, 2000

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON BANKING AND FINANCIAL SERVICES,
Washington, DC.

The committee met, pursuant to call, at 10:05 a.m., in room 2128, Rayburn House Office Building, Hon. James A. Leach, [chairman of the committee], presiding.

Present: Chairman Leach; Representatives Roukema, Bereuter, Lucas, Barr, Kelly, Ryun, Biggert, Terry, Green, LaFalce, C. Maloney of New York, Gutierrez, Ackerman, Bentsen, J. Maloney of Connecticut, Hooley, Carson, Lee, Inslee, Schakowsky, Moore, Gonzalez, Jones and Capuano.

Chairman LEACH. The hearing will come to order.

The committee meets today to hear testimony on H.R. 4585, the Medical Financial Privacy Protection Act, and other measures in this arena which are designed to protect the most sensitive information about an individual that is held by a financial firm.

Before summarizing this proposal, let me review the legislative background of the issue.

Last year, in consideration of H.R. 10, the Financial Services Modernization Act, this committee for the first time in the long history of bank reform legislation approved a privacy package. In addition to erecting privacy shields for American financial services customers, including a ban on the transfer of information to third-party telemarketers and a clampdown on identity theft, the bill that left this committee contained a provision that would have walled off the medical records held by an insurance company from other affiliates of a financial services holding company, as well as non-affiliated third parties.

H.R. 10 passed the House with the strongest privacy protections ever incorporated into banking law, importantly including the medical privacy provisions that originated in our committee. Later, however, at the request of the Administration and the insistence of the Minority party on the floor that the issue be addressed through Executive action rather than legislation, the medical privacy provisions were dropped from the final version of the bill.

Now it appears a consensus is developing among the interested parties in the Government on the desirability of moving forward with a legislative approach to medical privacy. In this regard, the language of H.R. 4585 is consistent with the medical privacy recommendations forwarded to Congress by the Treasury Department six weeks ago and responds to the concerns outlined by the

President in his April 30 speech at the Eastern Michigan University in Ypsilanti. And in an important disclosure area that deals with information concerning mental health or conditions, H.R. 4585 goes beyond the Administration's recommendations.

The legislation is also consistent with the industry accord announced last week. The industry is to be complimented for agreeing to voluntarily provide a credible degree of privacy protection of the medical records of their customers. Some would even contend that, because of this voluntary agreement and because of the industry's general record of safeguarding medical records, any legislation represents a solution seeking a problem.

Yet the background of legislative concern in this area relates less to any history of past industry abuse or of new financial industry organization, but rather to the implications of modern information technology as it relates to the new genetic sciences. So much more can now be known about and predicted about individuals based upon medical testing that it is important to put common sense restraints in place before temptingly improper industrial practices begin.

The major provisions of the bill, H.R. 4585, which is the principal subject matter of the hearing are as follows:

Financial institutions will be required to obtain customer's consent, or opt-in, before disclosing individually identifiable health information to an affiliate or non-affiliated third party.

A financial institution will be prohibited from obtaining or using individually identifiable health information in deciding whether to issue credit, unless the prospective borrower expressly consents.

Information relating to mental health or mental condition will be singled out for particular protection with separate and specific customer consent required to disclose such information and special policies developed by regulators to protect its confidentiality.

Consumers will be given the right to inspect, copy and correct individually identifiable health information that is under the control of a financial institution.

Strict limitation will be placed on the redisclosure and reuse of individually identifiable health information legitimately obtained by a financial institution.

And nothing will be done to modify, limit or supersede medical privacy standards promulgated by the Secretary of Health and Human Services pursuant to authority granted under the Health Insurance Portability and Accountability Act.

The approach contemplated in H.R. 4585 is designed to augment the privacy provisions of the financial modernization bill passed last year. Rules to implement those privacy protections are in the process of being implemented by the Executive Branch, and I believe I can speak for all Members of the committee in encouraging that regulators should move expeditiously so all Americans can be more secure in the privacy of their financial information.

Before hearing today from the Administration, Government officials, industry representatives and privacy groups on their perspectives, let me ask Mr. LaFalce if he has any opening comments.

[The prepared statement of Hon. James A. Leach can be found on page 66 in the appendix.]

Mr. LAFALCE. Mr. Chairman, I do. The difficulty is I think we have about five minutes left to vote, and I don't know if I would be able to get my five minutes in.

Chairman LEACH. The gentleman is correct. We have a little more than that, but I think that if he doesn't want to be interrupted it would be better to move to the vote. I think that is very appropriate.

Let me say we have a very, very long set of panels, and we have votes expected on the floor actively today, and so it will be my intent to limit opening statements for five or six or seven more minutes and then turn immediately to our first witness.

The hearing then will be in recess pending the vote.

[Recess.]

Chairman LEACH. The hearing will reconvene, and Mr. LaFalce is recognized.

Mr. LAFALCE. I thank the Chairman.

This morning's hearing continues our committee's work on financial privacy which we began two years ago when Chairman Leach introduced legislation, which I co-sponsored, to prohibit pretext calling and other privacy abuses and I introduced a related bill to impose obligations on financial institutions to protect the confidentiality of customer information. I am very pleased to say that both proposals were enacted into law as part of last year's financial modernization legislation in much the same form as they were originally introduced.

This year, I introduced H.R. 4380, a comprehensive proposal developed in concert with the Administration to address financial privacy broadly. I think it is an excellent bill. H.R. 4584, which the Chairman has introduced, addresses one of the issues dealt with in H.R. 4380, medical privacy, by restricting the use and disclosure of financial institutions of personally identifiable health and medical information. This is an issue not included in the legislation adopted last year, and not adequately addressed in pending HHS privacy regulations.

Both H.R. 4380 and H.R. 4585 reflect the growing bipartisan recognition that the privacy protections adopted last year do not go far enough in assuring that sensitive personal information will be protected by financial institutions and that additional protections must be enacted.

The issue of medical financial privacy eluded us last year. Our committee did adopt a narrow provision to restrict the use of health information in connection with credit decisions. That was replaced by a broader bipartisan financial privacy proposal on the House floor.

The Commerce Committee had a proposal that would restrict the disclosure of health-related information by insurance companies. It was referred to as the Ganske Provision. And that was omitted in conference in response to strong bipartisan concerns that it might preempt pending HHS privacy regulations, preempt stronger State medical privacy laws, and permit widespread sharing of sensitive health data under broad exceptions for many different things. So all the major medical and hospital associations, all the patient and consumer groups and privacy advocates agreed that the Ganske

language at that time created greater potential privacy problems than it resolved. And so both H.R. 4585 and H.R. 4380 have meritorious proposals on medical privacy.

In many respects, H.R. 4585 is comparable to the medical privacy provisions of H.R. 4380; in some respects, it does differ. And some of those respects where it differs I have some difficulties, but I am sure those difficulties can be worked out in probably a manager's amendment.

But the primary limitation of H.R. 4585 is not what it does. It is rather what it doesn't do. It applies only to medical and health information, which we must do and is extremely important. But the higher standard of protection for the sharing of consumer profiles and lists should apply to all sensitive health and financial information, and the new protections for consumer access and correction should apply to all sensitive financial information, and the stronger standards for reuse and redisclosure of information should apply to all sensitive financial information and not just health or medical information.

So, in short, I think H.R. 4585 is a very good effort, but I also think we need to do more. If consumers do not want their financial account information shared with affiliated companies without their knowledge, we need to do more. If consumers object to having their spending habits and product preferences—referred to as "profiling"—if they don't want these habits and preferences monitored and sold or shared for marketing purposes, we need to do more. If consumers don't want health and insurance information taken into consideration for investment or employment decisions, we need to do more. And if American consumers want to have the same privacy rights being given to European customers of United States institutions, we need to do more. And if consumers want the right to determine if their financial records are accurate and up-to-date, we need to do more.

So I urge today's witnesses not to confine themselves solely to the topic of the very important and necessary need of medical privacy legislation that is before us, but I personally would welcome any comments on the broader aspects of the Administration's privacy proposals either as contained in H.R. 4380 or any other proposals that are needed to assure the strongest possible privacy protections for American consumers.

I want to especially thank the Chairman for accommodating my request for witnesses for today's hearing, all of whom will be on Panel IV, and I join with the Chairman in welcoming all of today's witnesses. I thank the Chair.

[The prepared statement of Hon. John J. LaFalce can be found on page 71 in the appendix.]

Chairman LEACH. Thank you, John.

What I would like to do in limiting opening statements is limit it to the Chairman and Ranking Member of the subcommittee of jurisdictions.

Mrs. ROUKEMA. I thank you, Mr. Chairman. I will be brief and have the full text of my opening statement in the record.

I would just make a couple of observations here. As you know, we in the subcommittee held hearings last year on these subjects, including not only financial, but also medical privacy; and, as you

have already noted, we have to go farther than what was in the Gramm-Leach-Bliley bill; and that is quite appropriate.

I want to endorse everything you have previously stated on that subject. Clearly, today we are opening up the door and continuing what we did in the subcommittee with respect to exploring medical privacy, and really the financial and medical privacy are interrelated, and we have to come to terms with them. Of course, we don't have the rules and the regulations yet evaluated. It is too early for that. But we hopefully will begin to evaluate those regulatory rules by this July, or certainly September.

I am questioning, however, what the status is and the scope of the medical privacy standards that were being developed or should be developed by HHS under the Health Insurance Portability and Accountability Act. I don't think that they have been clearly enunciated. I think you made reference to that. Perhaps we will find out something more today. If not today, then I certainly would expect to make a formal inquiry with them for a complete report.

In addition, Mr. Chairman, I also want to say, although we do have the American Psychiatric Association here today and at least one other group that is directly involved—that are direct health-related organizations, I do plan to inquire with at least the American Medical Association, the Health Care Leadership Council, and the National Alliance for the Mentally Ill and other medical groups, because I think it is absolutely appropriate for us to have those who deal on a daily basis with medical issues in the immediate world with patients to have more input into our deliberations here. So I will be making those inquiries, and we can discuss it another time whether or not it will be appropriate to make that a formal part of our report.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Marge Roukema can be found on page 77 in the appendix.]

Chairman LEACH. Thank you, Mrs. Roukema.

Mr. Gensler, please.

STATEMENT OF HON. GARY GENSLER, UNDER SECRETARY FOR DOMESTIC FINANCE, DEPARTMENT OF THE TREASURY

Mr. GENSLER. Thank you, Mr. Chairman, Ranking Member LaFalce, Members of the committee. Thank you for having me here to talk about this critical issue of privacy.

I am also honored to have with me my second daughter. Lee Gensler is right behind me. I know that Congressman Capuano last week, when I did this with my other daughter, thought it might be bordering on, as he said, "child abuse," but, believe it or not, my second daughter also wanted to come and see how Congress works.

Chairman LEACH. On behalf of the committee, we give a special welcome to Ms. Lee Gensler.

Ms. Gensler, if you would like to sit next to your father, you would be welcome so to do. If you are like my family, we know that the rule is in inverse proportion to age. Please, Ms. Gensler.

Mr. GENSLER. She thanks you.

I am pleased to have the opportunity to talk about the Chairman's bill, H.R. 4585, and privacy in general. My written testimony that I hope to submit for the record, but let me just summarize—

does address four areas: first, the need for privacy protections in the financial area; second, last year's advances in the Financial Modernization Act; thirdly, the President's comprehensive Consumer Financial Privacy Act initiative; and then, fourthly, medical privacy.

If I may just summarize briefly.

Many Americans increasingly feel their privacy threatened by those with whom they do business, particularly when it comes to privacy around their financial information. We are in the midst of extraordinary changes in the financial industry. These changes are brought about, we think, in three ways: first, integration and consolidation, in part brought on by the Gramm-Leach-Bliley Act, but largely brought on by consumers and markets; second, advances in technology—clear and dramatic changes in technology; and, thirdly, the explosion of the use of electronic payments and electronic receipts—where transactions can be measured and recorded.

Last year's efforts were very significant, and we believe the Congress and the Administration worked together in a bipartisan way to move privacy protections forward in a constructive way around notice and choice, around third-party sharing, and about important protections beyond that. The Administration believes, however, that much more can be done and should be done to protect financial consumer privacy.

To that end, the President announced an important new legislative proposal in late April to provide Americans more fully with an effective financial privacy act. That legislation now before Congress is H.R. 4380, the Consumer Financial Privacy Act, and is a balanced, comprehensive approach to financial privacy, providing important new rights and protections while addressing some of the shortcomings in last year's bill.

A central Administration principle is that the greater the sensitivity of the data and the possible harm from misuse, the greater should be the level of privacy protection; and the Chairman, I think, recognizes that with regard to the medical area. The Administration's proposals, therefore, call for the strongest protections in two highly sensitive areas: first, the sharing of medical information, as, again, the Chairman's bill also recognizes; and, second, the use of detailed personal spending habits information about an individual consumer—the entire list of all of our spending, where we spend our money, how we spend our money, a whole portrait of an individual.

For other financial information, however, the Administration's proposal would give consumers the opportunity only to opt-out: the first two opt-in, but other areas just opt-out before a financial services firm can share that information for marketing purposes. This would, in essence, extend the protections of last year's bill to affiliate sharing.

But, importantly, the Administration recognizes that there is a bulk of information sharing, a shared type of information sharing, if I might call it that, that provides for consumers to understand that sharing, but not have a choice to opt-out; and that is for risk management, that is for fraud, that is for law enforcement, many of the provisions this Congress wrestled with last year. The Administration suggests adding one very important component to that—

that would help consumers and help the economy—which is related to consolidated statements and consolidated call-in centers to facilitate, again, the consumers.

We are pleased so many Members of Congress have supported this approach. We especially thank Ranking Member LaFalce, who sponsored this approach, and led this with many Members of this committee.

Let me now just turn to, more specifically, to medical privacy. We are deeply committed to providing consumers control and rigorous safeguards with regard to medical privacy. Under the terms of the HIPAA law, which was passed by Congress in 1996, and the rules under them, privacy protections apply to covered entities, and I think that this was one of the questions raised earlier. Covered entities are only health providers, health plans, and health clearinghouses so, thus, includes health insurers. They do not cover life insurers, do not cover property and casualty insurers, do not cover auto insurers and many disability insurance programs, all of which, I would say, are now financial institutions and defined as such under the Financial Modernization Act of last year.

The proposals offered last year addressed some of the issues, but could have seriously undermined the crucial medical privacy initiatives, such as preempting the HIPAA roles and the other issues that I think Congressman LaFalce outlined in his opening statement.

HHS is right now in the midst of a rule-writing process. They put out the proposed rules last fall, and the President committed in his State of the Union to finish these rules this year. They are right now in the midst of rule writing and have received many comments on those critical, important rules. But, again, those rules would not be able to cover many financial institutions such as life insurance companies, property and casualty, disability insurers, because of the nature of the 1996 Act.

Mr. Chairman, by convening this hearing you have focused attention on the important issues surrounding financial privacy and medical privacy. While we continue to believe it is necessary to seek legislation that provides comprehensive privacy protections, your bill offers a starting point for consideration of the issues that will be very important and truly important for a privacy regime. Let me say there is common ground between your bill and the Administration's proposal regarding financial privacy. H.R. 4585 does differ in some significant respects, and I would like to just highlight two of those for you today.

First, the scope of the bill. We believe that financial privacy legislation should address the full range of financial privacy issues, as the Administration proposal does. H.R. 4585, while sharing many of the Administration's views on medical privacy, is in contrast to a narrow bill that does not address issues beyond medical privacy. Medical privacy within the financial services industry is vitally important as only one aspect we believe in moving forward.

Second, with regard to the bill itself on medical privacy, in one regard, with regard to receipt and use provisions, these are the provisions that will prohibit, unless a consumer consents, a financial institution to receive or use medical information. They are limited to the extension of credit or a loan. Thus, the Chairman's bill sug-

gests that, before you receive or use medical information in extension of credit or loan, you have to get specific opt-in by the consumer.

We share that view, but we believe that it is important to have that receipt or use limitation broader than just for the extension of a credit or a loan. If a financial firm is giving investment advice, should it be able to get information from a life insurance affiliate before it decides on the investment advice? If a financial firm is providing auto insurance, should it be able to reach to the insurance company and get the medical information—or even if it is providing travel services, which, by the way, under the Financial Modernization Act, includes travel agencies as part of financial services? Before giving travel services, should it be able to reach next door to an affiliate to get medical information? We think that the receipt and use provisions are strong, but should be broadened and should apply to the broad set of financial services and products.

In conclusion, Mr. Chairman, we thank you for providing this forum to discuss this critically important issue. This hearing provides a starting point for a thorough consideration of the range of privacy issues raised by changes in technology and our financial markets. This is truly an historic opportunity to get financial privacy right, to put in place all of the protections that American citizens want and need.

We recognize the special sensitivity of personal medical information, and we support having effective laws that match the sensitivity of that data. At the same time, we should also address the vital issues that were included in the Consumer Financial Privacy Act. We think to do otherwise is to miss out on an opportunity and that we can work together and address these issues. We look forward to working with you and thank you again.

[The prepared statement of Hon. Gary Gensler can be found on page 78 in the appendix.]

Chairman LEACH. Well, thank you very much, Secretary Gensler. Thank you for your loyal support.

Ms. Lee.

Mrs. Roukema.

Mrs. ROUKEMA. Mr. Chairman, you caught me a little off guard here. I expected you and Mr. LaFalce to first be speaking.

Let me ask this, Mr. Gensler. You state that the President has pledged that the final medical privacy regulations will be issued this year. Pursuant to the authority of HIPAA, which I referenced, the 1996 law, and I referenced that in my opening statement, but these rules would apply only to certain—as I understand it, only to certain, "covered entities" and would not apply to most financial institutions. I believe in your opening statement, although I was interrupted at one point, necessarily interrupted, that you made reference to the question of not being included in terms of affiliation in Gramm-Leach-Bliley, but maybe you could amplify that.

But the point is, there is not specificity as to what would apply and what would not apply to the financial institutions, but I am really deeply concerned, because they are integrated. They are in some ways integrated. Aside from that, we have to go beyond necessarily in this legislation, but what can be done has not yet been done under existing law. So could you amplify please with more

specificity as to what we can expect and how you recommend we close those loopholes?

Mr. GENSLER. The bill that was passed by Congress in 1996 provided that if Congress were unable to pass further legislation within a three-year period, then the President was authorized through HHS to put in place these regulations. Those were proposed last fall. They only cover health providers, health care plans and health clearinghouses. That is what the bill said. And thus they cover health insurers, but not life insurers, not property and casualty like auto insurers and the like. So, what this committee has before it in the Chairman's bill and in the Ranking Member's bill, does cover those other financial entities.

Mrs. ROUKEMA. I believe I understand that. Those are the covered entities that you were defining.

Mr. GENSLER. Right. Congress defined those in 1996; and, thus, the HHS rules are unable to address the other sharing that may go on.

Mrs. ROUKEMA. I certainly realize that, but are they now being instituted or are they still in the comment period?

Mr. GENSLER. They have closed the comment period. They got, I think, literally thousands of comments.

Mrs. ROUKEMA. But they are not instituted as yet?

Mr. GENSLER. The final rules would become effective later this year and I think under the statute had two years for implementation.

Mrs. ROUKEMA. You see no conflict here by any means either under regulatory authority or with the affiliation regulation and the law where this legislation will certainly close those loopholes in a defined manner. Yes?

Mr. GENSLER. I think both the Chairman and the Ranking Member's bill recognizes the HIPAA rules and has, I would say, sort of a safe harbor for that, and this is additive, thus, I think that is appropriate in both of these bills.

Mrs. ROUKEMA. In terms of additive, you don't see any conflict coming up there in terms of a legal question within the affiliation structure, none whatsoever?

Mr. GENSLER. I don't believe so.

Mrs. ROUKEMA. I thank the Treasury Secretary.

Mr. GENSLER. Thank you.

Chairman LEACH. Thank you, Mrs. Roukema.

Mr. LaFalce.

Mr. LAFALCE. Thank you very much.

First of all, Mr. Gensler, let me commend you on the outstanding job you have been doing in your role as Assistant Secretary of the Treasury for Domestic Finance and for the fine testimony you have given us today.

As I understand it, having worked with you very closely in the development of the Administration's broader, more comprehensive financial privacy package, you believe that the bill before us today, Mr. Leach's bill, is a good bill, but you have difficulty with: A, its scope, which we will talk about later; and second, with certain details which I have said I think can be worked out and perhaps even by a manager's amendment. Let's deal with those details first. Could you expand upon those just a bit more? If we were only to

consider the bill before us, forget about scope, how would you want it improved?

Mr. GENSLER. I think we have made some very good progress together since last year's debate and identified a new way to address financial medical privacy, and it is in the receipt or use of that information. If some part of a financial institution under the Chairman's bill, a bank in extending a mortgage or in extending an auto loan, receives or uses information from an affiliate or a third party, in fact, it can't do that if it is medical information unless it has specific consent from the consumer.

We applaud that provision. We think that is right. It stops the use or receipt of that information. Our comment is that we think that in the President's bill we went broader, that it was not only in the extension of a mortgage or an auto loan, but it was the extension of other financial services. And, as I highlighted, we think that whether you are extending investment advice or extending an auto loan, for instance, a financial institution should not without the consumer's specific consent receive, use medical information from one of your affiliates. Again, the Chairman's bill did include many of the provisions on access, on reuse, on personal spending habits around medical.

Mr. LAFALCE. I haven't had a dialogue with the Chairman on this, but I feel confident this is something we could come to closure on. What I am concerned about is that we not lose sight of the fact that there are broader issues, too, which we have attempted to address in a broader bill. I made a statement, and I would ask you to comment on them seriatim. If consumers don't want their financial account information shared with affiliated companies without their knowledge, would we need to do more than H.R. 4580?

Mr. GENSLER. We think that we should not stop at medical. We think that there are broader issues, particularly around personal spending habits, that are enhanced and have a heightened level of sensitivity that ought to be included, and the American people want included, in their zone of privacy.

Mr. LAFALCE. If we want to stop profiling, would we need to do more than H.R. 4580?

Mr. GENSLER. Yes, we would.

Mr. LAFALCE. If we want to give American consumers the same privacy rights that European consumers of United States financial institutions have, wouldn't we have to go further?

Mr. GENSLER. The answer is yes, particularly as it relates to affiliate sharing.

Mr. LAFALCE. Good. I just wanted to set the stage that I don't think that we should arbitrarily—let me scratch the word arbitrarily—I don't think we should prejudge the legislative approach we should take to our problems. I think we ought to hear what the scope of the problems are and then come in with legislation to address it, rather than just start out with something narrow.

I don't want to turn down something that deals in a good manner with one piece of the problem. By the same token, I don't want to make a prejudgment that we can only deal with one piece of the problem. I prefer to go for a larger, more comprehensive approach. I thank you.

Chairman LEACH. Thank you, John.

Mr. Bereuter.

Mr. BEREUTER. Thank you very much, Mr. Chairman.

Secretary Gensler, one of the exceptions to the opt-out provisions of the Gramm-Leach-Bliley Act authorized disclosure of information by insurance companies to State guaranty funds. Neither the Administration's bill nor H.R. 4585 extends the State guaranty fund exception to the opt-in provisions applicable to disclosure of the health information. Several of the industry witnesses bring up this point or will bring it up before the committee later in at least their written testimony. What is the Administration's rationale in omitting the State guaranty fund exception from the medical privacy opt-in proposal?

May I ask a second question, too? It relates to a concern among some financial institutions of a significant regulatory burden that could be imposed when they have only a one-time transaction with respect to a person, for example, wiring money by Western Union one time only.

Would you care to respond to both of those two items?

Mr. GENSLER. Yes, Congressman. In terms of the State guarantee point, what was not clear to us in the last four months in developing the bill was why there might be a need for individual medical records with regard to that exemption that you rightly point out is in Gramm-Leach. So we have not heard a specific reason why individual medical records are needed. Again, we look forward to working with this committee if there is something that we have overlooked, but nothing has come to our attention.

In terms of the second issue, there are provisions even under the Act last year and the rules that are now put in place in terms of one-time transactions to really lessen, as you say, burdens or lessen the requirements on a one-time transaction. Somebody goes up and uses an ATM machine, and it is not their bank's ATM machine. We took a lot of public comment on that. We know the regulators modified that in the final rule. We have not changed that in the President's bill or in the Chairman's bill. I don't think we have changed that aspect moving forward.

Mr. BEREUTER. Thank you. But I gather you are willing to look at possible changes in that area if, in fact, it can be demonstrated.

Mr. GENSLER. We look forward to working with this committee in trying to move a product forward that addresses the needs of the American people.

Mr. BEREUTER. Thank you. We will see if there is a case that needs to be made and then make it.

Thank you, Mr. Chairman.

Chairman LEACH. Thank you, Mr. Bereuter.

Mrs. Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman. I request that my opening comments be placed in the record.

Chairman LEACH. Without objection, and without objection any Member who wants to make opening comments.

Mrs. MALONEY. Thank you, Mr. Gensler, for appearing before the committee again and bringing your daughter Lee.

First, I want to thank you and the Administration for making consumer privacy one of your highest priorities. I know that this issue is critically important to Secretary Summers. He has spoken

before the committee on it and to the Vice President, who just spoke out last week on this issue.

I would like to ask you, my district is the home of a number of large institutions, especially hospitals, and could you comment on your interpretation of the bill as it relates to patient service? Could the opt-in provisions prevent medical staff from having the most timely access to information that they may need for emergency patients or are additional exemptions necessary?

Mr. GENSLER. I think it is a very critical issue. We do not believe so.

This is also a very critical issue that HHS is addressing in their medical regulations in terms of sharing of information, and we know they have gotten comment on it. But we don't believe so, and it certainly would not be the intent either in rule or in law that a patient in an emergency room setting would have that difficulty. It is the intent, though, to limit information sharing in the advancement of a financial product—again, investment advice or other financial products where there is not that emergency situation.

Mrs. MALONEY. I certainly support the Chairman's bill, but I am disappointed that it only—and that we are considering today only the area that it addresses, which is medical privacy, and I wish that it had a broader scope, particularly the broader bill that Mr. LaFalce has put forward that includes really the Administration's policies that they put forward.

I am concerned that U.S. citizens are really treated differently than many of our trading partners in our global economy, specifically in Europe where they have much stronger consumer privacy; and given that much of the opposition to consumer privacy protection is based on their costs and operational difficulty, why should U.S. law be weaker than that of our trading partners?

Mr. GENSLER. Well, this Administration stands for strong consumer privacy protections, particularly with regard to financial privacy. I think that, as you have seen in the Ranking Member's bill and the President's full support, it would bring us to those standards which we think are again balanced, whereby industry would have a base of information they could share, but then the sensitive information would have higher standards surrounding them.

Mrs. MALONEY. I certainly hope that the Chairman will have a hearing on the Administration's proposal, because these extended and more complete consumer protections are very, very important.

I have spoken to many industry representatives that tell me, particularly in the health industry, that they are willing to go forward and provide this consumer privacy to their customers, particularly on medical information, and why is legislation necessary if companies are willing to take these voluntary measures?

Mr. GENSLER. Well, we think, as the Chairman said in his opening remarks, that this is important in moving forward not only to prevent actions even if they are not rampant today, but also to instill confidence in our financial systems. Something fundamentally is changing around commerce today, not just banking, but overall, and it is the internet, and it is electronic commerce. And to instill confidence in the internet and instill confidence in the financial system, we think that fundamental consumer protection, funda-

mental privacy rights, actually promotes the economy by building confidence. So, if they are going to do it anyway, instilling it in law doesn't take anything away, but it builds confidence.

Mrs. MALONEY. Actually, as we speak, the e-commerce bill is on the floor that would break down yet another barrier for signatures for contracts, which is a very important bill which underscores the point that you are making.

Mr. GENSLER. We have worked successfully with this Congress on that bill, and that is a very important bill to move forward electronic commerce. But, again, that bill is done in a way that was sensitive to consumer needs to build the confidence in this new economy.

Mrs. MALONEY. My time has expired. Thank you very much for your testimony.

[The prepared statement of Hon. Carolyn B. Maloney can be found on page 74 in the appendix.]

Chairman LEACH. Thank you.

Mrs. Kelly.

Mrs. KELLY. Thank you, Mr. Chairman. I just have a couple of very quick questions here.

There has been some concern expressed that the provision that we have here threatens to impose a significant regulatory burden on financial institutions that have to respond. I wonder how the Administration responds to those concerns. The regulatory burden on the financial institutions is something that I think we really need to think about. I wonder how you respond to that concern?

Mr. GENSLER. I think that the bill before you today and the President's bill build on the provisions in the Gramm-Leach-Bliley Act so they are meant to be consistent and build upon that.

But there are two areas that people have raised. One, they have said there might be a burden, because you limit information in the great new economy that we have. We think not because there is a base of information that can be shared as long as it is restricted to reuse, but shared for risk management, fraud, for securitization; and we have actually added a provision in our proposal for consolidated account statements, an important provision. So there is a base that provides all that information.

What the Administration is saying is to market to an individual that we should provide individuals the right to opt-out, to say "I might not want to be marketed to," and then for medical and for complete profiles of an individual that it would be an opt-in. We think that those limited provisions are important, actually, to promote the financial industry.

Mrs. KELLY. Your testimony just now, though, didn't include the problems with one-time transactions. There are some serious problems I think there in terms of the regulatory burden that will be imposed on the financial institutions. People have a one-time transaction. I think that needs to be considered. Do you think the Administration would consider possible changes to address something like that?

Mr. GENSLER. You are right, the bill and the testimony actually do not take up the issue. It is precisely consistent with what Congress enacted last year; and in that regard, the rules that were put in place had less of a responsibility on the financial institution for

those one-time transactions in terms of, in essence, the opt-out for third-party sharing and the like. I believe that the regulators address that in their final rule. I am not aware of further comments that came up.

Mrs. KELLY. Would the Administration be open to a change?

Mr. GENSLER. Well, again, we look forward to working with this committee, moving forward on getting the best privacy protections for consumers, but also those that are balanced and work for the economy.

Mrs. KELLY. Are you aware of any specific instances or is the Administration aware of any specific instances where banks have denied credit based on medical information about the loan applicant, whether it has been gotten from an affiliate or from a non-affiliated third party? Do you know of any instance like that?

Mr. GENSLER. While I am not familiar with them, we are in a world that is really new in terms of the ability to have databases and to bring together data across a financial institution in a way that it is important to put these protections in, as I think the Chairman had said, before commercial interests take over. There is a temptation there that is really there, and we think it is best to address this now and, in addition, to instill the confidence in the system that I think will promote the banking system in itself.

Mrs. KELLY. If I understand correctly, you are talking about instilling confidence by drafting a law, but you don't have any specific instances that you can talk about where banks have denied credit to people in those instances.

Mr. GENSLER. I think, with all respect, we see no reason to allow somebody in extending a mortgage to look into your personal medical history unless they are asking that of all those applicants of the mortgage and unless they are asking your permission. We cannot see any reason why that should be allowed.

Mrs. KELLY. I don't think anybody does, except—anybody wants that, really, but, on the other hand, I think it is important that we not draft laws and pass laws when there is not a need for a law.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Sue W. Kelly can be found on page 70 in the appendix.]

Chairman LEACH. Thank you, Sue.

Mr. Ackerman.

Mr. Bentsen.

Mr. BENTSEN. Thank you, Mr. Chairman.

Mr. Gensler, in reading your testimony as it relates specifically to the health information issue, would the Administration be supportive of H.R. 4585 if the receipt and use provisions were similar to what is in the President's bill, including the requirement that it is the same requirement on all customers? Is that your main holdup with respect to the health issue?

I understand that you want—that the Administration believes that the Congress ought to go further in revisiting the entire Title V of the Gramm-Leach-Bliley Act, but if we were just to focus on health, which was effectively carved out at the end of the process last year, would those be the main changes you would be looking at for H.R. 4585?

Mr. GENSLER. You are correct to say those would be the main changes in terms of the health provisions of H.R. 4585. The Administration feels that it is important to move forward in these other areas, that to share all of the ways that Congressman Bentsen spends his money, where you spend it, how you spend it, a complete list of that, to be able to share that without your affirmative consent is not an appropriate standard. So we feel that it is best to be comprehensive, and we look forward to working with this committee and the Congress to achieve that.

Mr. BENTSEN. I understand where Mr. LaFalce wants to go as well. It seems to me that a very strong case can be made that, with respect to health information or medical privacy, that we did not go as far in that area as we did in other areas of financial privacy in the Gramm-Leach-Bliley Act and were we not able to muster support for a broader bill, would it not be appropriate to at least plug this one gap in the medical privacy? I realize your aide is providing you answers there—but, to plug this one gap with a bill like H.R. 4585, would the Administration—I know you don't want to give up the whole thing yet, but don't you think that if there was one thing we could get done this year, isn't this an area where Gramm-Leach-Bliley was failing in medical privacy as compared to other areas?

Mr. GENSLER. We share this committee's view that that is a gap. It is a gap I think in part created because we have a new situation where insurance companies can affiliate with banks. Before the Gramm-Leach bill, that was not legally permissible. But, I would say, Congressman, I still feel strongly that we should address these other issues, that it is important. Some issues that actually benefit industry—for example, to allow for consolidated calling centers—we think very importantly also benefit consumers, not only through getting greater services—like consolidated call-in centers would give greater services—but also in terms of giving greater confidence and protection around the sharing of the specially sensitive information.

Mr. BENTSEN. H.R. 4585, as the Administration reads it, would enforcement of this be in the same way as the other financial privacy parts of Gramm-Leach-Bliley are? And the Chairman has pointed out that it would not preempt or supersede the HHS's role under the HIPAA law. Does the Administration agree with that interpretation? Do you believe in any way this would preempt the Secretary of HHS or HHS or the HIPAA law? Are you comfortable with how that section is drafted?

Mr. GENSLER. Let me make sure. I think the answer to both parts of your question are yes, that the Chairman's language and the language in H.R. 4380 do not supersede HIPAA or HHS, as we can see, in any way.

Mr. BENTSEN. Finally, does this bill—and the Chairman may answer this. But does this bill or does your bill preempt State law or does it follow along the same track that Gramm-Leach-Bliley did that gave the States the predominant role in setting privacy standards?

Mr. GENSLER. It sort of adds to Gramm-Leach-Bliley, and so you are familiar with those provisions. In these bills there is no state-

ment on preemption, thus leaving in place the regime that we have prior to these bills.

Mr. BENTSEN. Thank you.

Thank you, Mr. Chairman.

Chairman LEACH. Mr. Lucas.

Mrs. Biggert.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Mr. Gensler, with this bill and concerning Worker's Compensation and automobile insurance, both of which deal with, number one, timely access to health or medical records, timely receipt of that, do you think this would cause delay in obtaining the relevant health data needed by worker's comp to proceed with claims and in the auto insurance, which also deals with indemnifying consumers from medical losses? I see a delay perhaps in worker's comp cases. What if the consumer actually refused to opt-in to provide their medical records in a case which questions their claim?

Mr. GENSLER. We don't believe that it would delay. But, also, if in any way when we think through this together that would be an issue, we would look at what technical issues needed to be added. We don't think so.

And I would add, because it allows for specific opt-in product-by-product, you could put a specific opt-in exception in cases that are necessary around providing the medical services or Worker's Compensation and the like, if it was medical services or disability.

Mrs. BIGGERT. That would apply then to maybe auto insurance?

Mr. GENSLER. It could; but, again, we don't think that either bill limits the timely payments under auto insurance. Because, again, if you have an accident, that is the time you share the medical information.

Mrs. BIGGERT. And then as far as the provisions for opting in and Gramm-Leach has the opt-out, is this going to be confusing for when you opt-in, you opt-out? Is this something that we need to deal with?

Mr. GENSLER. We don't think so. There are many provisions already in law that are opt-in—video rental, under the Federal Privacy Act, certain provisions under FCRA—the Fair Credit Reporting Act—in terms of sharing your credit report with employers and the like. So there are standards this Congress has put in place that are opt-ins where there is especially sensitive information. Even under HIPAA it is effectively a consent or opt-in for health and medical information under HIPAA, but, unfortunately, it only applies to health insurers and not other insurers.

Mrs. BIGGERT. A U.S. Supreme Court refused to hear an appeal by a Federal Appeals Court ruling in Colorado that struck down as unconstitutional regulations promulgated by the FCC that restricted intracarrier sharing of certain customer information, and what they looked at specifically was the opt-in provisions, which seemed to be somewhat similar to this bill and the Administration proposals. Have you looked at that case?

Mr. GENSLER. I haven't personally. Let me just ask. I think I am going to get an expert answer.

Let me just say, we have been working with the Department of Justice around all the Administration privacy proposals and focused on the 10th Circuit opinion, and believe that the Administra-

tion's bill in terms of its opt-in provisions, and I think this would also count for the Chairman's bill, but I don't know that DOJ has had the same amount of time, are constitutional, even in light of the 10th Circuit opinion.

Mrs. BIGGERT. Thank you.

Thank you, Mr. Chairman.

Chairman LEACH. Thank you, Mrs. Biggert.

Mr. Ackerman.

Mr. ACKERMAN. Thank you very much, Mr. Chairman. I did have a question, Mr. Secretary. On a previous question, did I understand you to say that you would be supportive of an exemption for one-time transactions as it might be burdensome.

Mr. GENSLER. I think what I said, in terms of the regulations under last year's law, we think they put in place a different set of obligations on those one-time transactions. We think they were effective. We are not aware of comments that have come in subsequent to that final rule. What I also said is we look forward to working with this committee on broad comprehensive privacy and moving broad comprehensive privacy forward related to financial privacy. If there is a specific issue, then it would be rightly taken up in that comprehensive bill. And we would be open to looking at appropriate issues to help protect consumers, but also to foster commerce.

Mr. ACKERMAN. In your view, would somebody undergoing a medical examination as a prospective insured under health insurance, would that be considered a one-time transaction? Well, as we don't have right now in place a medical financial privacy law, it is more in the prospective I think that you would probably be asking it, but in terms of the Administration's approach, if you are conducting an exam for life insurance that is specific to that product, and if the life insurer is asking it of all customers under the President's proposal, as long as it is asked of all customers and you are consenting to it, you are having the physical, so you are personally consenting to it, then that moves forward.

What we are trying to protect is that that health information is not then used by some affiliate for some other financial product, a separate financial product.

Mr. ACKERMAN. What about for the same financial product? To give you a specific example of that, that would be of assistance to you in thinking this through, a person goes for a medical exam for life insurance and they make a determination that the person tested positive for HIV. And they decide not to insure the person and they decide not to disclose it to the person who was tested, and they decide to post it using a secret code on the internet made available to insurance companies so that every other insurance company who belonged to the association, knowing the code will understand that this person tested positive and would therefore be warned not to issue insurance. Would you be in favor of that one-time exclusion under those circumstances?

Mr. GENSLER. Absolutely not, sir. Absolutely not. The only thing that, trying to highlight, I think, in your earlier question, is that nothing in these bills would prohibit a life insurance company from requesting that you have a physical exam for that product provided by that life insurer. But that life insurer should not, and I think

Americans would all agree, be able to share that information with others or post it on the internet.

Mr. ACKERMAN. Not every insurance company agrees with that. Thank you, Mr. Chairman.

Chairman LEACH. Thank you, Mr. Ackerman.

Mr. Terry, did you seek recognition?

Mr. TERRY. No.

Chairman LEACH. Ms. Hooley.

Ms. HOOLEY. Thank you, Mr. Chairman. Thank you, Mr. Gensler. Thank you for bringing your daughter. I think that is great.

Mr. GENSLER. Thank you.

Ms. HOOLEY. Most of my questions have been asked, but there are still a couple I have. Do we need any special provisions or anything different that deals with mental health? Do you put that in the same category as all other health?

Mr. GENSLER. Well, the Chairman's bill actually has a specific provision with regard to mental health, and it was an enhancement, in fact, in the President's bill to have a specific consent with regard to mental health, and we think it probably is appropriate to have an additional protection in a separate category, and we look forward to working with this committee if there are other enhancements in that specific field.

Ms. HOOLEY. Another question is, tell me one more time what is the difference in this bill that enhances that privacy regulation over what the Secretary of Health and Human Services has come up with?

Mr. GENSLER. The Secretary of Health and Human Services has limited authority, limited because the 1996 law that people are referring to as HIPAA only related to "covered entities"—health providers, health plans, and health clearinghouses. Life insurers are not a covered entity. Disability insurers are not a covered entity. Auto insurers, property and casualty are all non-covered entities. Banks, by the way, are not covered entities. So she's moving forward and the President is moving forward the best they can, but it is within that law.

Ms. HOOLEY. Then lastly, I know your bill is looking at how do we protect consumers. Have you done any looking at what it costs financial institutions to implement these proposals?

Mr. GENSLER. Well, I know that the regulators did some on the Gramm-Leach provisions, but in terms of moving this bill forward, it again just builds on the basis of the Gramm-Leach provisions for notice and choice, and importantly, a choice with regard to medical in the Chairman's bill. But we have tried, I think, in both bills, to just build upon the same regimes and the same methodologies that I say went through public comment. I think there were 2,600 comments that came in on the earlier provisions, most of which were constructively addressed.

Ms. HOOLEY. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEACH. Thank you.

Ms. Carson, did you wish to be recognized?

Ms. CARSON. Not right now. Thank you.

Chairman LEACH. Mr. Inslee.

Mr. INSLEE. Thank you, Mr. Chairman. I want to thank the Chair for following through on this important issue. I know the Chair feels strongly about closing this massive loophole and getting this resolved. I am very hopeful that we will do that this year, and the other Chamber will follow our lead. I appreciate the Chair's advancing this at this time. But I think it is very important to note that I feel that our job, even if we resolve this issue, and I am confident we will, at least in this committee, that there are really massive imperfections in the Gramm-Leach bill that we ought to address this month, and to date, we have not had any encouraging signs that we will have hearings either in full committee or subcommittee on closing the affiliate sharing loophole, and that causes me great concern, because I can tell you that since we last addressed the issue of privacy in this committee, this issue has taken off like a rocket in America.

We had the first sort of inkling of that last fall when I first brought an amendment in Gramm-Leach-Bliley to address this whole privacy issue, and I think all of us Members of Congress since then have learned that there is probably no issue in America today that is growing in people's anxiety levels than the loss of privacy in this country. I think since we passed the Gramm-Leach bill, that has continued to grow exponentially. You can't pass a magazine stand without reading or pick up a newspaper today, and I can echo those comments that are on Main Street.

So the question comes, when are we going to address this affiliate sharing issue and when will this committee have hearings to do that? I suppose we could wait until the next Congress to address that if we felt we didn't have enough information to know whether there is a problem today. But I have to ask this question: Do we have to wait till the next Congress to figure out that companies are going to share private personal financial information against our interests, against our specific directions with their various affiliates under Gramm-Leach? We do not have to wait till the next Congress to know that that is going to happen as soon as it is legally permissible.

Second, do we have to wait that when our constituents find out that that is going on, that they are going to be outraged? Do we have to wait till the next Congress to figure that out? I suggest we do not have to wait to know that Americans are going to be outraged about these telemarketing gambits that are going on, sharing their personal private information. We don't have to wait till the next Congress to figure that out.

Lastly, do we have to figure out in the next Congress how to deal with this issue? I don't think there is any reason we are going to learn something between now and the next Congress. So I feel very strongly that this committee ought to have hearings, this Congress, on the affiliate sharing issue and the issue of opt-in/opt-out, which remains in contention. The Chair has shown leadership in bringing this to this committee, and I am just hopeful that we will have an opportunity to further address this affiliate sharing issue in Congress.

Having said that, Mr. Gensler, my soap box, I would just ask if there is anything you would like to add on the timing of this discussion?

Mr. GENSLER. Congressman Inslee, we applaud your leadership on this issue. It was very good to work with you on the digital signature bill as well, which is such an important issue for this Nation.

We share your views. We think that there is no time to address this issue like now. This is all going one way, it seems. One of my colleagues earlier today said that Congress is conducting five different hearings, that the Administration is talking about privacy in one realm or another this week. It just gives a sense of the potency of this to the American people. I think that we have had a thoughtful balanced approach about affiliate sharing. We come out on the side of the debate. The Administration comes out, as you do, that there should be some choice; that regarding notice and choice, there is no distinction between affiliates and third parties, and that the one issue that industry has raised—and we have dealt with, is consolidated call-in centers and consolidated statements. They already had what is known as the 502 E exceptions in the Gramm-Leach bill, which is a series of eight important exceptions, and it is time to move on.

And I think we believe that credit card companies should not be able to share a complete list of how you spend your money, where you spend the money. In essence, a total portrait of you as an individual, without you having the right to say "Yes, you can share that and tell somebody the complete search and the complete portrait on Congressman Inslee."

Mr. INSLEE. That perhaps could be some interesting reading, I suppose.

Thank you, Mr. Gensler. Thank you, Mr. Chairman, for bringing this to our attention. I am just hopeful that the Chair can see to allow this committee to address this issue and not have to wait for new Members of Congress. I think there will be some new Members of Congress here perhaps because of this issue, but we shouldn't have to wait for them, and we ought to, on a bipartisan basis, move forward in this regard. Thank you.

Chairman LEACH. The Chair would like to thank the gentleman for his advice and the Secretary as well. I would also like to thank both the gentleman and the Secretary for switching to the Chair's position, and now supporting in a more timely basis, the medical privacy issue. I am glad, having sought delay on that issue last year, you are now in favor of moving forthrightly at this time.

Mr. Moore.

Mr. MOORE. Mr. Chairman, I don't have any further questions of Mr. Gensler. I do appreciate your work in this area, and I am hopeful that we can, as Mr. Inslee pointed out, expand it at some point beyond just medical privacy and financial privacy, but internet privacy and a lot of other issues that are of great concern, I think, to the American people. Thank you.

Chairman LEACH. Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much.

Quickly a couple of questions. As you have indicated, one's medical records, medical information and personal spending habits, information profiles, would be two categories of information that would rise to the level of this special zone of privacy. I think that may be the term which really equates to opt-in. That is the distinc-

tion in mind, anyway. I am wondering what other type of information, in your opinion, would rise again to the level which would place it in this special "zone of privacy?"

Mr. GENSLER. The two areas I think you highlighted were those two areas, medical information, and then the complete portrait, the complete spending habits. Those were the only two that we thought would be at that enhanced level, and in essence, the burden would be on the provider of services to get your consent. Another area—just marketing—the burden, in essence, would be on the consumer to fill out the form and send it back in, but we thought that that is less sensitive information, and thus the burden, more appropriately, is on the consumer.

Mr. GONZALEZ. In all your discussions, though, nothing else has entered those discussions that, again, make it this type of treatment on the opt-in standard.

Mr. GENSLER. That is correct. As I noted earlier, Congress has had opt-in for other provisions, whether it is in the Telecommunications Act or video rentals and other areas that Congress has seen that as an appropriate means of protecting a zone of privacy.

Mr. GONZALEZ. The second question relates to the HHS standards which would apply to health plans, health care clearinghouses and certain health care providers, as you pointed out. Then we have this bill here, H.R. 4585, that would encompass financial institutions. Who have we left out?

Mr. GENSLER. I am not quick enough to think, but in terms of medical—this addresses financial institutions. I am sure there are some institutions that are neither financial nor health care providers.

Mr. GONZALEZ. That is my point. I guess this bill is going to continue the piecemeal approach to privacy legislation. I understand we approach privacy many times in many ways, and maybe the final outcome is we will have one bill that maybe can address all the different activities. The reason, obviously, is that you have certain entities that may have shared activities, for instance, that would subject them to one set of rules, and possibly another set of rules, thus creating confusion. That is why I was just asking you, is there anything that you see now that needs to be addressed differently in this bill? Should some other enterprise, some other activity, some other business, be included or deleted?

Mr. GENSLER. The President has laid out and the Administration has felt strongly that there are three areas broadly that are appropriate to address statutorily and that is medical, financial, and children's online. Those are the three broad areas that he and the Vice President have laid out a number of times, and the Administration has moved forward and worked successfully with the Congress on the Children's Online Privacy Act some time ago, worked successfully, even last year, on the financial bill, even though we think we should do more.

Mr. LAFALCE. I wonder if the gentleman from Texas would yield for a question.

Mr. GONZALEZ. Of course.

Mr. LAFALCE. Mr. Gensler has been assisted in his testimony by a relative of his, and it is my understanding that you have been assisted in your questioning on this issue that it is an appropriate

zone of privacy by a relative of yours, an attorney from San Antonio, who has prepared quite an outstanding book dealing with the issue of zones of privacy, which I hope you would share with the Members of the committee.

Mr. GONZALEZ. Not at this time, because it would be a lengthy discourse, I guarantee you. Thank you.

That is all I have. Thank you very much, Mr. Chairman.

Chairman LEACH. Mr. Lucas, do you seek recognition?

Mr. LUCAS. No.

Chairman LEACH. Mr. Capuano.

Mr. CAPUANO. Thank you, Mr. Chairman.

Mr. Gensler, I just have a couple of questions. I guess one is purely educational, as far as I am concerned. Under the current situation, the current laws, oftentimes I pick up the local papers and I read on a regular basis probably several times a week about a prominent figure in the community coming up with some medical problems, admitted into the hospital for this, admitted into the hospital for that, being treated in an experimental way for this problem, that problem.

Under current situations, is that person protected from any retribution, potential—maybe a better word can be used—any reaction from the financial community? Could that person have his loans or her loans pulled, have them called, be denied if they are in the middle of getting a mortgage, and a banking executive happens to read right now that they are getting treatment for some heart anomaly?

Mr. GENSLER. I just wanted to check. No, there are no Federal statutes in place that would limit that at all.

Mr. CAPUANO. I didn't think there were, but I wasn't sure. I want to make sure. I guess I would like at some point some people to take a look at that as well. I am not so sure it is easy to put your arms around. I am not so sure it is something you can address, but it is something, there should be lines. I think there should be lines, especially people in my world, in your world. There is nothing I do that is private. Nothing. And people have websites up and pretty much everybody here, probably on you, too, telling all the terrible things I did just yesterday, never mind the rest of my life, and I would be concerned deeply if my family were negatively impacted.

It is not just politicians, anybody in the public realm is subject to that, and it would concern me if there were no limits whatsoever on—it is one thing, freedom of speech to say whatever you want to say. I understand all that. But you know as well as I do, if you go right now, if you are admitted into a hospital for a checkup right now, you know darn well the likelihood is pretty good that we'll be reading about it in the paper tomorrow.

I don't think that that is something we should just ignore. It is one thing to focus on the immediate problem in front of us. I think that is all well and good. It is a big step forward, but I don't want to lose sight of the bigger issue as well.

Shifting gears, the only other issue I have I heard earlier there is always concern about passing laws that were not needed, we are not sure we need them. I am not interested in the morality, not interested in the ethics, I am not interested in the social aspects of privacy. I have my own opinions on that. That is all well and good.

I am interested in the financial aspects. In the banking world, do you think that the banking world would be better served financially if Congress were to sit back on this issue or any other issue and not speak, let it go until there is a problem and then react after the businesses have invested probably millions of dollars in software, millions of dollars in personnel, millions of dollars in mailing and telephone centers, and so forth, and so forth, and so forth, because maybe I am wrong, but my estimation is that once the first financial institution starts sharing medical information, even though the others will say "It is morally reprehensible, it is terrible, we will never do that." But the first time they save money or they make money, someone else is going to fall in line. And eventually we are going to end.

It strikes me as financially better for the financial services community if we can set the rules now, let them know what the rules are going to be now rather than waiting for some situation to arise, and I don't think any ordinary American thinks that it won't happen if we do nothing. Something will happen and we will overreact and have wasted millions of dollars, millions of hours of personnel time and all the problems that are associated with changing business practices.

I guess I just wonder, do you think I am completely off the wall? I don't mind being off the wall. That is what I do. Or do you think there is in legitimacy to that concern?

Mr. GENSLER. We think that it is fundamentally important to address this issue for consumers and for the banking system. We think it, as we said earlier, not only instills confidence, but gets ahead of an issue that could be—it is like an attractive nuisance. It's too tempting, frankly. And having been in Commerce, I could never imagine that any of my former partners would do anything on this, but I think it is attractive, and it is there and I think we should address it.

Mr. CAPUANO. I never would have thought that so many people would be calling me in the middle of the night twenty years ago trying to sell me another credit card after I have 400 in my pocket already. But that attractive nuisance is just unavoidable when there is money to be made. I understand that. I ask the question having already formed my opinion. I think it is good business practices for Congress on issues such as this to set the bars now to save the time, the trouble, the money that is involved in following down what I think will end up being a dead end.

Mr. GENSLER. It is also, as we change so rapidly, what we want to do is adopt the new information age, as we move from sort of the industrial age to the information age. The President said in his speech in Ypsilanti, he said, when we moved from an agricultural age to an industrial age, it was important to adopt new laws at that time, to put in place really the progress and to expand to the full middle class the nature of the industrial age as we moved into the 20th Century. As he said better than I could, we need to do the same as we move into the information age, and put in and adopt laws to help us move and promote, for all Americans, the success moving forward.

Mr. CAPUANO. As a little footnote to that, I think it is well put that there were many people in those days that objected to the pro-

posed laws at the time as overbearing, overreaching. We don't need them. We are doing fine without them. It is not a new story. It is an old story and I think it clearly worked well for this country, for the American people in the past transitions, and I think it will work well here. Thank you.

Chairman LEACH. Thank you.

Ms. Schakowsky.

Ms. SCHAKOWSKY. No, thank you.

Chairman LEACH. I think that is the last questioner. Let me just briefly opine, because we are in the realm of privacy, and several constitutional issues have been raised, and the Chair is willing to suggest that Freedom of Information requests do not apply to the notes passed from Ms. Lee Gensler to her father. In any regard, we thank you very much, Gary.

Mr. GENSLER. Thank you, Mr. Chairman.

Chairman LEACH. Our second panel is composed also of a single witness. Ms. Kathleen Sebelius, who is Commissioner of Insurance for the State of Kansas and Vice President of the National Association of Insurance Commissioners. I would like to ask Mr. Ryun if he would like to make any welcoming remarks.

Mr. RYUN. Mr. Chairman, first of all, I am sorry I missed the opening statements and didn't have an opportunity to welcome my Insurance Commissioner, Kathleen Sebelius. But I do want to thank her for coming today. She has been an advocate for the medical privacy of Kansas. She has been recognized for her efforts in Kansas, and certainly by the National Association, and I welcome her testimony to do what we can to ensure that all Americans have the kind of medical privacy that we are looking to protect in light of the Gramm-Leach-Bliley bill, and I want to thank her for the opportunity to say something, and welcome. Thank you for coming today.

Chairman LEACH. Thank you, Mr. Ryun.

Mr. Moore, would you like to comment as well?

Mr. MOORE. Thank you. Mr. Chairman, again, I congratulate you on your good work, on convening this hearing, and the bill that you drafted. I also appreciate the opportunity to extend some brief remarks to welcome Insurance Commissioner Kathleen Sebelius here.

Kathleen has a very interesting background. She comes from a bipartisan political family. Her father was Governor of Ohio. Her father-in-law was a former Member of Congress from Kansas. Her husband is now nominated to be a United States District Court judge in Kansas.

I am very, very pleased to have Kathleen here today. She was first elected in 1994 and reelected in 1998 as Kansas Insurance Commissioner, and previously served four terms in the Kansas House of Representatives. She currently is, as I think the Chairman indicated, Vice President of the National Association of Insurance Commissioners, and is Chair of the Working Group on Privacy. That is the capacity she appears before our committee today.

She was recently recognized as a renaissance regulator by the June issue of *Best's Review*, a national magazine focusing on insurance issues. They observed, and I thought this was very interesting, that she was able, in the last five years, to eliminate almost

half of the regulations on insurance in the State of Kansas. She has established a reputation as a national leader on health insurance issues and is leading the NAIC effort to develop uniform regulations that balance privacy for individuals against insurers' business needs for consumer information. I often turn to Kathleen for advice and counsel, and I really am pleased to have her before this committee today, and she's always very able to render thoughtful and insightful testimony and I appreciate that.

Welcome, Kathleen.

Chairman LEACH. Thank you very much. It looks like you come with near perfect credentials, Mrs. Sebelius, although some of us would prefer that you took your father-in-law's, rather than your father's, party. You are very welcome and please proceed as you see fit.

STATEMENT OF HON. KATHLEEN SEBELIUS, COMMISSIONER OF INSURANCE, STATE OF KANSAS; VICE PRESIDENT, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Ms. SEBELIUS. Thank you, Mr. Chairman. It is nice to be here and nice to be here with half of our congressional delegation, my own Congressman and my friend, Congressman Moore. I appreciate the opportunity to be here and also bring you greetings, Mr. Chairman, from your own insurance commissioner, Terry Vaughan, who is now serving as Secretary-Treasurer of our association. We have just finished four days of insurance meetings, our summer meetings, so she said to be sure to extend her greetings to you.

Unfortunately, my colleague, Glenn Pomeroy, who is a former President of our association from North Dakota, and whose brother serves with you in the House, is stuck in Bismarck. Planes couldn't get out of Minneapolis last night, and couldn't get Mr. Pomeroy to Washington today, so he apologizes for his absence at this hearing.

What I would like to do before I talk a bit about health privacy, Mr. Chair, is just use a few minutes to give you an update on the way insurance regulators are moving to comply with the features of Gramm-Leach-Bliley, which is a fairly sweeping change for regulators. I think it is safe to say that the passage of this bill focused attention and mobilized my colleagues from around the country to move very quickly to comply with various aspects of that bill. In just three short months we have had 50 State regulators sign a statement of intent on implementation features which have a comprehensive buy-in for uniform standards across the country on a variety of issues, including a more efficient and uniform regulation of the financial services marketplace.

We have nine different commissioner-level working groups in place to implement the law in areas like privacy, agent licensing and speed to market for insurance products. The Gramm-Leach-Bliley has created expectations, and frankly, our goal is to exceed these expectations. We feel it gives us a good framework to move to a 21st Century regulatory system and we have been hard at work doing that.

Having said that, I also appreciate the opportunity to testify on the very important issue of health information privacy and the new legislation before this committee, H.R. 4585. This will be the sixth time during the course of the 106th Congress that we have come

to testify on health privacy, and are pleased to see that there is a recognition in this proposal, as there is in the President's proposal, to recognize that an unintended consequence of Gramm-Leach-Bliley is the fact that a consumer's sensitive health information can now be shared freely without distinction from other sorts of financial information.

Although, as you all know, health privacy wasn't specifically included in the language of Gramm-Leach-Bliley, the Federal regulations changed that landscape, because the definition of financial information now includes health information. Unfortunately, given the framework of the original bill, the law doesn't provide the kind of stringent protection that we feel, and most consumers feel, is needed for sensitive health information.

Mr. Chair, the regulators were very sensitive to the pleas from the industry that the financial portion of the regulations that we were mandated to promulgate for insurers across this country, would not put them at a competitive disadvantage with their colleagues. As such, our initial draft regulations follow the guideline set out by Gramm-Leach-Bliley. On the other hand, the commissioners felt unanimously that health information needed to be treated differently, should be treated differently, and we are in the process of crafting regulations which would separate out health information and provide for the same kind of opt-in standard that you have provided in this bill.

Specifically, I would like to highlight a couple of areas where there is a lot of consistency between our approach and the approach of H.R. 4585. First is the basic recognition that health information should be treated differently than financial information. Second, it should be treated with more protection than financial information with an opt-in standard across the board.

Again, the NAIC framework has been always to say it is the information that should be protected, not necessarily the entity that has that information. So in our prior models and in our current regulations, we don't delineate between a worker's compensation company, an auto insurance company, a life insurance company or a health insurer who may have health-sensitive information. We think it is the information that deserves the same kind of protection. And it should be across the board with financial institutions, again, recognized by your bill.

These aspects of your bill mirror the standing NAIC policy, and we applaud your efforts in amending Gramm-Leach-Bliley to include these important protections. As I said, we have been fairly consistent on this. We had a model in 1980, a general privacy model, that recognized an opt-in standard. We updated that model in 1998 specifically for health information, again recognizing an opt-in standard. And we are currently at work drafting the model regulations which we will urge our colleagues across the country to implement in compliance with the Gramm-Leach-Bliley regulations, and which, again, have an opt-in standard for health information.

Frankly, it is probably preferable if Congress acts on this measure, because that is a way to ensure that the standard is in place simultaneously around the country and doesn't need to wait on a State-by-State implementation of the regulatory framework. It is

that framework that we are here to urge you to move forward on. We do have an accelerated timetable for finalizing our regulation. As you know, the Federal regulations were not final until mid-May of this year. We wanted to wait and see the framework of the final financial Federal regulations before we moved ahead, but we hope to have the final draft of the regulations for insurers ready by September, so States can move either with their own regulatory authority, or in next year's legislature, to put these in place.

As has already been discussed, a lot of what is in your bill mirrors the HHS regulations, but given the jurisdiction of Health and Human Services, a lot of entities who collect and hold sensitive financial information will not be covered by the regulations, which, at the earliest, I think are scheduled to be effective December of 2002.

So we are still a long way from seeing some sort of standard on health privacy regulations. Having said that, Mr. Chair, the insurance commissioners across this country look forward to working with this committee on this very important issue. We applaud separating health information, having an opt-in standard for health information, and urge you to move forward.

[The prepared statement of Hon. Kathleen Sebelius can be found on page 87 in the appendix.]

Chairman LEACH. Thank you very much, Ms. Sebelius.

Mrs. Roukema.

Mrs. ROUKEMA. Mr. Chairman, I am going to reserve my time. Thank you.

Chairman LEACH. Mr. Ryun.

Mr. RYUN. I would like to ask a question related to your testimony. Apparently, you share a very disturbing story with regard to a company that apparently shares a claimant's, if you will, prescription information with a pharmaceutical company. Then it tried to market those particular products to the customer's physician. Now, how often does this happen? Is this simply an isolated situation or is it rather frequent?

Ms. SEBELIUS. Frankly, Congressman Ryun, I can't enumerate the number of times. I chaired the Privacy Working Group that drafted our 1998 model, and that testimony was part of the hearing process that came forward. We heard a number of very disturbing pieces of testimony where bits of medical information were revealed, clearly not by the consumer, but by some entity collecting it.

I know that in my own situation, and I have had a gentleman in Atchison come up to me after a speech I gave on medical privacy, to say that he was terribly concerned, because he had just finished a series of tests which resulted in his diagnosis as an adult onset diabetic. Within about a week of that confirmation by the medical clinic, he began receiving bulk-rated syringe mailings, insulin alternative products, a variety of information. As he said to me, "I didn't put a bumper sticker on my car. I didn't put a sign in my yard that said 'guess what, I am a diabetic.' I didn't take an ad out in the *Atchison Globe*, but somebody in that chain of events did release my information, and I am now seen as a marketing tool."

He was quite unhappy with that, and unfortunately, I think it happens more often than we would like. I can't quantify around the country how many times it has gone on.

Mr. RYUN. What we are advocating here, do you think in this situation it would help solve part of this problem?

Ms. SEBELIUS. I think it would help greatly. As has already been raised by earlier questions to the Assistant Treasury Secretary, the combination of this bill, which is aimed at financial institutions, and the currently-pending Health and Human Services regulations, which cover a broader scope of health plans, providers, hospitals and medical information, creates a pretty substantial umbrella for those who are collecting and holding financial information to prohibit sharing without specific consumer consent.

Having said that, I think that our draft model, and certainly we would urge the committee when regulations will be drafted, creates large business exemptions. We recognize that insurers, for instance, need to process health information on a regular basis to pay Workers' Compensation claims, analyze a PIP auto carrier, or underwrite a product, and those were recognized within the regulations that we would put forward. It doesn't impede the business of insurance, but it does preclude you from sharing information, selling it, or marketing it for other reasons without the consumer saying it is OK to do so.

Mr. RYUN. Thank you.

Mr. Chairman, thank you.

Chairman LEACH. Thank you.

John.

Mr. LAFALCE. Thank you very much.

Ms. Sebelius, I was discussing with the Chairman earlier privately the importance of trying to find the appropriate role for both the Federal and the State governments on so many different issues with respect to bank charters, with respect to charters of credit unions, and so forth. One of the areas we are going to have to grapple with in the future is the appropriate role of Federal legislation as opposed to State legislation in protecting privacy. Do you think, as a starting point philosophically, that Federal law should: A, be preemptive of the States?; or B, just establish minimal standards, but not preclude the States from adopting their own additional consumer standards?

Ms. SEBELIUS. Congressman, the views of the association that I am here to represent, and my own personal view, are that the kind of Federal floor issue, particularly in this area, is very appropriate. As you know, State law has——

Mr. LAFALCE. When you say Federal floor, I think you mean it should not be preemptive; is that correct?

Ms. SEBELIUS. That is correct. The way I understand it, at least the overall framework of Gramm-Leach-Bliley, particularly in the privacy areas, is that it does recognize the opportunity for States to be more consumer friendly, more restrictive. States have, over the course of fifty years, developed various kinds of health privacy standards often tied to some very specific kinds of laws in place, certain kinds of Workers' Compensation systems which are tracked, or medical tests which are done in a certain State.

While I think we have said consistently in the past that we think there is a clear role for Congress, we believe it is appropriate to have national privacy standards governing national definitions, governing a large area of this. Our caution about blanket preemption, particularly in the privacy arena, is the unintended consequences of various kinds of particular State laws which could be wiped out and could actually put consumers steps behind where they are right now. So we are very cautious about blanket preemptions.

Having said that, I think we would encourage moving forward with broad guidelines that are nationally implemented and nationally known. I don't want to go skiing in Colorado and have a different set of recordkeeping for my medical records there than in Kansas. I don't think that serves the consumer well and it certainly is very difficult for an industry to operate under. In the major areas I think setting standards and saying these should be nationalized are very appropriate.

Mr. LAFALCE. I think that is basically the approach we took last year, financial services modernization. I think that is the approach both that the Chairman and I have taken in our respective bills further addressing the issue.

Now, you mentioned that the NAIC has come up with some model standards, model legislation, and you pointed out the similarities between the model legislation you come up with and the bill introduced by the Chairman dealing with the issue of medical privacy. My first question is, did your model standards only deal with the issue of medical privacy, or did you consider other issues?

Ms. SEBELIUS. We attached two pieces of model legislation to, I think, the written comments, Congressman LaFalce. The 1998 model, which is attached, specifically deals with health information privacy and recognizes a need to carve out that area. The earlier model, which I think was 1980, dealt with across-the-board information kept by insurers, and also had an opt-in standard for non-affiliates to receive any kind of information, financial or health, collected by insurers.

So we have sort of dealt with both areas. But the 1998—the newest area, was dealing very specifically with health in lots of detail.

Mr. LAFALCE. Has the NAIC reconsidered its 1980 and adopted it anew, or you have just not gone back, that is two decades ago. There were a few advances in technology and electronics and market usage in the past two decades.

Ms. SEBELIUS. Right now we are in the process of trying to comply with the mandate to develop regulations as functional insurers to apply privacy regulations for insurance companies across the country. We are developing a model regulation in two phases. The first, which is what is underway right now, and hopefully will be completed by September, is an interim regulation. We have actually drafted it with a sunset clause and have attempted to mirror, on the financial side, the standards that are in Gramm-Leach-Bliley; no disclosure among the affiliates, and an opt-out for non-affiliates, with the exception of health information where we are drafting a more stringent standard.

I will share with you that there are a number of colleagues of mine who feel very strongly that we should revisit even those ear-

lier standards for financial entities, because those are not strong enough and are not protective enough of consumer interests on the financial side, and we see that as phase two.

Mr. LAFALCE. I think it would be helpful, mutually helpful, if we kept in close touch on these developments, because we could both gain.

If I could go back, though. You addressed similarities between your 1998 standard and H.R. 4580, and there are similarities between that, the bill that I introduced working in concert with the Administration. But Mr. Gensler also pointed out some concerns. One of them was scope, just didn't deal with other issues. Aside from scope is and not dealing with other issues, there was some particular difficulties that I think can be addressed. Are there any dissimilarities between your model standards and H.R. 4580 that you think we should address, and particularly what about the dissimilarities that Mr. Gensler pointed out in particular?

Ms. SEBELIUS. I don't want to misspeak, because I am not as familiar as I should be with all the details of H.R. 4585, but I think that there really aren't any inconsistencies. In fact, the draft of the bill, our privacy model, I think, could be used as regulations to implement the bill that is before you.

Mr. LAFALCE. What I would ask then, do you think you could, in writing, make comment on the specific details that Assistant Secretary Gensler had with H.R. 6320?

Ms. SEBELIUS. I would be glad to.

Mr. LAFALCE. Thank you. Thank you, Mr. Chair.

Chairman LEACH. Mr. Bentsen, do you seek recognition?

Mr. BENTSEN. Thank you, Mr. Chairman. I think you have one on your side down there.

Chairman LEACH. Mrs. Biggert.

Mrs. BIGGERT. Yes. Thank you, Mr. Bentsen. Thank you, Mr. Chairman.

You mentioned several times the Workers' Compensation and the auto insurance issue, which I had asked before. Do you think there needs to be something put into this bill to clarify that issue?

Ms. SEBELIUS. Congresswoman, I think that as I read this, there is nothing inconsistent in here with having a regulation that would give the kind of—I think you are going to need very specific business exemptions. It is part of what is contained in our privacy model which is attached. We really tried, again from the insurance side, to think through carefully what are the areas that insurers, both property, casualty and health, are involved in where health information needs to be shared.

So I think it could be addressed in the regulations. I think it would need to be addressed in the regulations, and perhaps some notice in the bill could do that. To not impede the business of insurance specifically, would be a good notice in the overall bill. I don't think the draft of the bill is inconsistent with providing those various business exemptions.

Mrs. BIGGERT. The other issue that was discussed earlier was the State guarantee funds and how they operate. Could you explain that a little bit to me, and then whether there should be some clarification as to that in this bill also.

Ms. SEBELIUS. I think that, again, they would be covered in a broad business exemption. I am not quite sure, and I know that is part of the ACLI testimony, exactly what it is in terms of the health arena that a guaranty fund would receive, which would be prohibited by this. As you probably all know, the guaranty funds assess and pay for claims left by an insolvent company.

So it is typically financial information which is gathered and exchanged, but if this would somehow impede that flow of information, we would certainly not favor that, and I think it could be easily provided for by an additional business exemption.

Mrs. BIGGERT. Thank you. Maybe just briefly also, since I have some time left, could you just tell what are the real benefits for consumers? Are they heightened or are they lessened, and how does this really benefit a single consumer?

Ms. SEBELIUS. I think most people believe that their personal health history is probably the most sensitive personal information they have. It seems to me that financial institutions may actually be enhanced in a role with consumers if they feel they are in a trusted position, and that the information they give to get a life insurance policy or pay an auto claim or get payment under a Workers' Compensation system is not going to be marketed to their disadvantage, is not going to be shared, and won't be used by a mortgage banker to not give them a home loan if they have some sort of wrong condition.

I think consumer confidence is key to any commercial dealings and we should be assuring consumers that this information is personal and private, it is protected, it needs to be exchanged for the commerce of doing the business of insurance and other financial entities, but it is not going to end up being used against them. It is not going to be something that will keep them from getting a loan, driving a car, operating in the normal business of their work day. I think that goes to the general good, and given the ease of collection and transfer of information, I think it is even more critical that the rules be clear at the outset. Consumers should know what is and is not going to happen to the information they give, and that there is some regulatory authority who is making sure that the companies follow those rules.

Mrs. BIGGERT. Thank you.

Thank you, Mr. Chairman.

Chairman LEACH. Thank you.

Mr. Bentsen.

Mr. BENTSEN. Thank you, Mr. Chairman.

I still remember what it was like to sit down on the lower row, so I wanted to make sure that Mrs. Biggert got her time in order.

Mrs. Sebelius, I want to ask you just a couple of questions. One is related to the testimony of the panel that will appear after you. I may not be able to be here for all of their testimony, and so I would hope and expect that they might respond to the question that I am going to pose for the record as well.

I haven't read all of the testimony, but in reading some of the testimony, a number of the organizations surprisingly would oppose provisions of the Leach bill as it relates to an opt-in requirement. They raise, I guess, this is my question. The reason that they raise is specifically with respect to employer-provided health ben-

efit plans that a restrictive opt-in requirement would make it difficult for the broker or the insurance provider to make adjustments in that plan with whoever I guess the carrier may be.

In your capacity as an insurance commissioner, as a regulator, do you see that as a problem; or is the initial agreement between the employee, employer, and insurance broker or underwriter with an opt-in at that point, would that be sufficient in giving the insurance carrier, broker, underwriter, whichever, the ability to make policy changes during the term of the agreement between them and the employer? Or is this a legitimate concern that these groups have?

Second of all, as part of that, they raised the question that this could become problematic between the insurance carrier—how the insurance carrier would work with a specific health care provider. I guess the example might be when you go into the emergency room and they are trying to verify your insurance coverage that there is a potential that this could block the transfer of information that would then make the provider unwilling to provide care for some particular reason.

And then I have another question after that.

Ms. SEBELIUS. Again, Congressman, I think that in the employee benefit plan arena, in the regulations that we are attempting to put in place right now covering insurers, we recognize that it isn't until information would be shared actually outside the general course of the business of insurance, that triggers the notice and the disclosure issue would be triggered.

I do think if the employee benefit area isn't carved specifically enough into this umbrella, it would be relatively easy to do that to include it in the broad business exemptions, because I think it is important to conduct the business of insurance. It is something that, again, I think we tried to do very carefully in that 1998 model when we came and urged Congress to look at it as one of the possibilities to meet the HIPAA standards that were at that point pending.

I think in the treatment area, again, the model attached to our testimony deals with all sorts of health care-related issues. If you go into an emergency room, where you would need to exchange information, what if you have an unconscious patient? How could he or she give disclosure? You don't want to shut down the possibility that they are going to get medical treatment if they can't get their records accessed. So that area is captured and I think very much present.

The way I read H.R. 4585, it is sort of the "20,000 view" level. It captures the major framework of what then would be implemented in specific regulations, and I think some of these issues and exemptions are not inconsistent with the framework. They would just need to be crafted into the regulations to make sure that they don't impede medical treatment.

You also don't want to impede research issues. There are broad exemptions, I think, needed for the research community to make sure you don't grind that to a halt by having too stringent rules on disclosure and nondisclosure for the business of insurance, but I don't think those are inconsistent with the notion that you are

not going to sell or market or share this information outside of doing some very specific activities.

Mr. BENTSEN. With the Chairman's indulgence, properly crafted, an opt-in could be properly crafted that would not impede the functioning of the insurance agent or broker, underwriter, you believe, and still provide this protection?

Ms. SEBELIUS. We believe that is true, and actually that is what we are going to advocate that our colleagues adopt as the standard for the insurance regulations which would meet the Gramm-Leach-Bliley mandate.

Mr. BENTSEN. I am going to have to leave, but I have one quick question, Ms. Madam Chairwoman. I would hope and expect that the other panel would address that issue when they testify.

Ms. SEBELIUS. They have been addressing me for the last four days, up close and personal. I am sure it will go on.

Mr. BENTSEN. They will be addressing us as well. You said in response to Mr. LaFalce, I think it was, the concern about a patchwork of State rules with respect to medical privacy protection, am I to understand that you would favor a Federal preemption of some sort or a uniform Federal standard as it relates to privacy rules, and that would be somewhat contrary to what we did in Gramm-Leach-Bliley?

Ms. SEBELIUS. Congressman Bentsen, I think that what I was trying to say is that when we testified in the period that the Kassebaum-Kennedy bill would have mandated Federal privacy action by August of 1999, that we urged Congress to move ahead and gave as part of that testimony what we thought would be a framework that would at least work well for insurers, which was the privacy model attached.

We have participated actively in commenting on the HHS regulations which are pending, and which eventually will at least be in place for the portion of the industry that I am familiar with that holds sensitive health information, but not the entire industry. I think it is appropriate that we have broad Federal standards in place simultaneously around the country with the same kind of definitions and same kind of protections for most of the areas of privacy.

The reason I have the caveat that I do is that there are literally thousands and thousands of State laws which have been in place for half a century, which have to do often with very particular kinds of State collections; databanks, Workers' Compensation systems, special tests. In Kansas, we do a special test for hearing of infants that is not nationally promulgated, but it is done specifically.

Wiping out in one fell swoop all of the State privacy laws which are in place in statutes could, I think, have some serious, unintended consequences for consumers, and that is what we are concerned about. I think broadly defining and outlining an area where the Rederal rules will be in place and would preempt State laws, makes sense. However, you need to be very cautious about what else you are wiping out in the State statutes.

Mr. BENTSEN. Thank you.

Thank you, Madam Chairwoman.

Mrs. ROUKEMA. [Presiding.] Thank you.

I do have a question, and that is, this bill or the Chairman's bill singles out for a particular protection information relating to mental health and/or mental condition, and it requires a separate and specific customer consent for disclosing such information.

Now, there is at least one other group or maybe others on the next panel that states in its testimony that a separate consent requirement for mental health information is not needed. I don't believe that you address this directly in your testimony, but I have a special interest in this concern. And of course on the next panel, we will also be having the American Psychiatric Association giving its own testimony, but I would appreciate having your input and your perspective on this particular question:

Should there be a specific separation? I believe there should be a specific customer consent as required in the bill. Could you please express yourself on the subject.

Ms. SEBELIUS. I am not sure I am able to give you a very complete answer on that. I can tell you that at least our old models and current regulations which are in place do not have specifically enhanced standards for mental health. And as far as I know, that was not a topic that was either addressed and rejected or accepted during the course of that process. I would just suggest that I think there could be other groups who come and say, you know, this sort of condition or illness may be equally——

Mrs. ROUKEMA. You are saying that your group has not specifically addressed that?

Ms. SEBELIUS. No. So I am not able——

Mrs. ROUKEMA. Can you explain in any way, even from your own perspective, how you could possibly separate one health issue from another?

Ms. SEBELIUS. The Chairman may be better able to answer that. The only issue that I am aware of and quite sensitive to is that there is a strong belief that mental health treatment carries with it such an extraordinary stigma that seeking treatment or seeking information about treatment, in and of itself may deter people from getting the help they need; and so having additional protections attached to confidentiality in that area may actually propel people to get much-needed help and treatment, and that makes sense to me.

Mrs. ROUKEMA. Thank you. I appreciate that.

Mr. Chairman, I have concluded my questioning. I appreciate your answer.

Chairman LEACH. [Presiding.] We have no further questions. We want to thank you very much, Mrs. Sebelius.

Ms. SEBELIUS. Thank you. We do look forward to continuing to work with the committee on this very critical issue. Thank you.

Chairman LEACH. Thank you.

Our third panel is composed of Richard K. Harding, who is the President-Elect of the American Psychiatric Association and Vice Chair of Clinical Affairs and Professor of Psychiatrics and Pediatrics at the University of South Carolina School of Medicine; my former colleague, Mr. Steve Bartlett, who is President of the Financial Services Roundtable; Mr. Don Brain, who is President of Lockton Benefit Company of Kansas City, Missouri, on behalf of the Independent Insurance Agents of America; Mr. Robert H. Rheel, Senior Vice President of Fireman's Fund, on behalf of Amer-

ican Insurance Association; Edward L. Yingling, Deputy Executive Vice President of the American Bankers Association; and Ms. Robbie Meyer, Senior Counsel, American Council of Life Insurance.

We will begin in the order of introduction. Let me welcome Professor Harding. Please.

STATEMENT OF DR. RICHARD K. HARDING, M.D., PRESIDENT-ELECT, AMERICAN PSYCHIATRIC ASSOCIATION, VICE CHAIR, CLINICAL AFFAIRS AND PROFESSOR OF PSYCHIATRICS AND PEDIATRICS, UNIVERSITY OF SOUTH CAROLINA SCHOOL OF MEDICINE

Mr. HARDING. Thank you, Chairman Leach, and thank you, Ranking Member LaFalce, Mrs. Roukema, and other Members of the committee for this opportunity to testify.

In addition to being at the University of South Carolina, I also served on the National Committee on Vital and Health Statistics, which advises the U.S. Secretary of HHS on medical privacy and medical information issues. But I am here today testifying as President-Elect of the American Psychiatric Association.

We now face what a bipartisan national panel of experts called a privacy health crisis. Many of us would say this represents somewhat of an understatement. As many of you saw probably a month or so ago on the newsstands, a magazine that said we know everything about you, because we live today in a 21st Century, cyberspace, high-definition, financial and health care system; but we also live with medical privacy laws that are more along the lines of the bygone black-and-white television era of Marcus Welby, M.D. While there are some very good corporate citizens who are voluntarily protecting patient privacy, such actions cannot substitute for statutory protections to ensure that all patients will enjoy needed confidentiality protections.

Your efforts, Mr. Chairman, as well as those of the Clinton Administration and Mr. LaFalce, to add needed privacy protections to the Financial Services Modernization Act is a critical, important first steps; and we strongly urge that you and your colleagues come together on a bipartisan basis and pass legislation to add privacy protections to the financial modernization law.

As we consider this issue today, I hope that each and every one of us in the room will think not only of the public policy issues involved, but also in terms of our own medical records and those of our family members. Medical records contain the most sensitive information about ourselves and our families, and as dedicated individuals in the financial services are, I can assure you that, as a patient, I want to make the choice myself as to whether my medical information is disclosed and I want the same thing for my family. The decision should not be made for us by a financial institution, insurance company, or a bank's mortgage lender. Disclosures of certain medical records information can jeopardize my career, our careers, our friendships, marriages and even our health.

How, you might ask, can financial modernization law affect medical privacy? Kind of simply put, the 1999 financial law insurers, including health and life insurers, can easily merge with banks and other financial companies. As a result in these large new holding companies, it is easy for any one of these entities to disclose med-

ical records information to a corporate affiliate such as a life insurance company, bank, mortgage lender, or credit card issuer. While I have no doubt that the new law will produce many benefits, we cannot ignore these privacy issues.

In addition to the importance of privacy and consumer transactions in our personal and professional lives, patient privacy is needed for physicians to provide the highest quality of care. It is often forgotten that doctor-patient confidentiality is an essential element for effective medical treatment. Without this high level of patient trust, many people will be deterred from seeking needed health care and for making a full and frank disclosure of information needed for this treatment. This is particularly true in psychiatric care.

In 1996, the Supreme Court, in the *Jaffe* v. *Redmond* decision, mental health information was decided to be so sensitive that additional privacy protections are needed for psychiatric treatment. The Court held that, "Effective psychotherapy depends upon the atmosphere of confidence and trust, and for this reason, the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment." We also were pleased with the 1999 U.S. Surgeon General's report on mental health research, and he reached a similar conclusion.

H.R. 4585 establishes a key principle for protecting the medical records held by financial services companies. The legislation would create a general rule, allowing patients to choose if their medical records will be disclosed to an affiliate company or nonaffiliated third parties. In these cases, companies would need the express written consent of the patient before disclosing medical records.

We strongly support this patient consent rule. I am equally enthusiastic about the bill's general rule ensuring the patient's mental health records not be disclosed without the patient's separate and specific consent.

I do believe there needs to be further discussion on the provisions implementing these general rules. No one wants the exceptions to the rule to swallow the rule. Yet, as currently drafted, do these provisions ensure that in the routine course of business, patient consent will be voluntary and noncoerced? This remains unclear. Likewise, the Secretary is now given new authority to create additional exceptions.

We look forward to working on these issues with you and your staff so the consumers in the real world enjoy meaningful new protections. Thank you for this opportunity to testify.

[The prepared statement of Dr. Richard K. Harding M.D., can be found on page 150 in the appendix.]

Chairman LEACH. Thank you very much, Professor Harding.

Congressman Bartlett.

STATEMENT OF HON. STEVEN BARTLETT, PRESIDENT, FINANCIAL SERVICES ROUNDTABLE

Mr. BARTLETT. Mr. Chairman, Madam Chairwoman, Members of the committee, I appreciate the chance to be here.

The Financial Services Roundtable, as you know, is a national association of 100 of the Nation's largest integrated financial serv-

ices firms, and as such, our member companies engage in banking, securities, insurance and other financial services activities.

Mr. Chairman, I am here to support your legislation, the purpose of the legislation, and to encourage you in this process. The Roundtable believes that protecting the confidentiality of health information that is in the possession of a financial institution is a matter that merits a uniform national policy. We supported similar legislation within Gramm-Leach-Bliley last year. We were disappointed when that legislation was deleted for reasons which we don't understand and, Mr. Chairman, we commend you on your leadership and consistency in promoting medical privacy. We support that legislation today, and we would support it in the future if it comes up in the future.

I want to say at the outset of this statement that the member companies that I represent—and so far as I know, most providers of financial services do not use or disclose health information derived from their customers other than for medical reasons or as otherwise intended by their customers. In other words, this issue is, at best, a potential loophole in our privacy laws, but it has quite a high emotional impact; and so even as a potential loophole, we believe it ought to be closed.

Mr. Chairman, overall, the members of the Roundtable believe that on the overall issue of sharing information, that the sharing of consumer information, in general, with affiliates and third parties can and generally does benefit consumers of financial services. Information-sharing between affiliates can permit, and with outside third parties can permit, an integrated firm to structure products and services that meet a customer's specific needs. We support, therefore, Gramm-Leach-Bliley's privacy protections, because it provides for both; the consumer benefits from appropriate information-sharing as well as protecting customer confidence.

However, we think that medical privacy is in a whole different category, that medical information is in a separate category and ought to be dealt with in a much stricter fashion in which the information should only be used for medical purposes, as it was intended.

We believe that medical institutions already have an obligation to maintain the confidentiality of medical records. That is an industry practice. We think it is covered by a myriad of State laws, regulations, various voluntary industry practices and court cases, and we think that what is called for here is a uniform national policy.

Mr. Chairman, having expressed my support for the bill in its proposed form, as well as in its purpose, the bill is not without some details that I believe need some change. We have worked with the member companies of all kinds of financial institutions, and we cite in our testimony a number of changes, some of which are highly significant, that I would put in the must-change category for this legislation to work.

Number one is, in Gramm-Leach-Bliley there are uniform exceptions to the confidentiality, and we think that those exceptions ought to be mirrored in medical privacy. First, and probably most important and the one most significant part of this whole legislation as it is currently drafted, is that the bill, as drafted, would not allow an insurance firm to share information with an insurance

rating advisory organization or a State insurance guaranty fund. If such information cannot be shared freely with the rating organizations, then the establishing of rates is not going to be possible.

Now, Mr. Chairman, perhaps there are some that believe we ought to eliminate rating of insurance and have one giant pool of 270 million Americans. I don't think that would be the intent of Congress; I don't think that would be the view of the majority of the American people. But if there is legislation to do that, we ought to have legislation that does that and not do it in a back door way through some other topic.

Second, the Gramm-Leach-Bliley provides other exceptions for the sharing of information with service providers which ought to continue in this legislation, and then other Gramm-Leach-Bliley exceptions. Mr. Chairman, we also believe that the consumers' access to correct their information has some ways, which I suggest in my written testimony, in which it can be drafted in a way that is more beneficial to consumers.

Next, we believe—and we have looked at the mental health provision. We think it is—we appreciate the intent of the mental health provision, but Mr. Chairman, I have to say that we believe that this legislation is a mere absolute prohibition of the use of medical information either physical or mental for uses that it wasn't intended for. We think that prohibition ought to apply equally to heart, lung, or mind and there is no particular reason that it ought to be separate.

Last, Mr. Chairman, I would say that we strongly believe there is a need for a national standard. Every State has a different law. There are multiple laws in different States. Only two States have a comprehensive law. There are twelve States that have model laws. All the others have a variety of laws, and then you have the Federal regulations on top of that and court cases on top of that.

We think this issue calls out for a national standard and we would encourage you to include that in the legislation.

[The prepared statement of Hon. Steven Bartlett can be found on page 155 in the appendix.]

Chairman LEACH. Thank you very much.

Mr. Brain.

STATEMENT OF DONALD C. BRAIN, JR., CPA; PRESIDENT, LOCKTON BENEFIT COMPANY, ON BEHALF OF THE INDEPENDENT INSURANCE AGENTS OF AMERICA

Mr. BRAIN. Thank you, Mr. Chairman, Members of the committee. My name is Don Brain. I am President of Lockton Benefit Group. We are the eleventh largest employee benefits consulting and brokerage firm in the country and the nearly 2000 employees of Lockton Benefit Group administer and work with clients all over the United States in their employee benefit programs.

Today I am appearing on behalf of the insurance agents and brokers, the nearly one million men and women who work in every part of the United States. These professionals are represented by the Independent Insurance Agents of America, IIAA, of the National Association of Insurance and Financial Advisors, formerly known as the National Association of Life Underwriters and the National Association of Professional Insurance Agents.

I serve as the IIAA's Governmental Affairs Committee member, the health care liaison to that committee. In addition to my role at Lockton Benefit Group, many of my associates are members of NAIFA and the Association of Health Insurance Advisors. NAIFA's conference is devoted exclusively to health insurance and benefits issues. All three associations represent health insurance professionals all over the country.

The associations that I am appearing on behalf of commend you for your leadership in bringing H.R. 4585, the Medical Financial Privacy Act, to this testimony today. We appreciate you holding this hearing and allowing us to testify on behalf of this legislation.

Perhaps there is no more important topic today in politics than the privacy of information, particularly medical information. At the outset we appreciate your leadership in this area and we appreciate your sensitivity in working with all three associations and their concerns to protect consumers' privacy regarding their medical histories.

The primary message that I want to relate to is that we want to work with you and Ranking Member LaFalce in making sure that this bill becomes the law of the land. The insurance agents fully support the overarching objective to protect individual sensitive health information and your approach to achieving that objective. At the same time insurance agents need to share information that they receive in the normal course of business and with health care and health care providers in order to provide a high level of service and the employee benefits of health care that we all want and need. Indeed, the vast majority of small businesses in the United States cannot afford separate health benefits, administration services or human resource services and rely on agents to fill those roles for their businesses.

From our perspective the only clarification that is necessary to ensure that the ongoing administration of employee benefit, employer-sponsored health benefit programs and Workers' Compensation programs is not disrupted in any way is to specifically provide that this information obtained in conjunction with the administration of these plans is not used for any purpose other than administration or securing information on a replacement plan.

Historically, the agent system has worked, has been the principal method of distribution for the life and health industry in the United States. Agents have been the essential link between the consumers and the insurance company providing services and products while educating consumers in how to manage risks and how to make informed choices about insurance purchases.

Dramatic increases in health costs over the last decade have caused the agents role to become even more important as part of the health equation. Agents fill roles in helping clients evaluate programs, educating them about information they need to make informed decisions, often making specific recommendations on programs that are designed to fill their needs and fit their budgets. We work with clients to ensure that accurate and complete information is available to secure the lowest possible premiums on their behalf in the marketplace. We keep in touch with them constantly to review and update periodic information and assist them in compliance requirements. We also review claims information and serve

as ombudsmen in their dealing and associates dealing with insurance companies. We assist business owners in communicating benefit packages to their employees.

At the outset, IIAA, NAIFA and PIA share the overarching concern about confidentiality of medical information. Although H.R. 4585 would help ensure that these confidentiality objectives are met, it must be clarified to make clear that these restrictions are not intended to interfere with the provision of employer-sponsored group health plans or Workers' Compensation programs in any way.

Without these clarifications that we have requested, the legislation would thus undoubtedly serve to both increase the costs of providing health care and reduce the number of options that employers would be able to consider. This would greatly undermine the level of care that many Americans are able to receive, and it would likely lead to a tremendous expansion in the number of un- or under-insured Americans.

In addition, many employers whose rates are established based on claims information rely on agents' review of the accuracy of the financial reports generated by third-party administrators and insurance companies to ensure that their claims information is accurately reported.

Thank you.

[The prepared statement of Donald C. Brain Jr. can be found on page 159 in the appendix.]

Chairman LEACH. Thank you very much, Mr. Brain.

Mr. Rheel.

STATEMENT OF ROBERT H. RHEEL, SENIOR VICE PRESIDENT, FIREMAN'S FUND, ON BEHALF OF THE AMERICAN INSURANCE ASSOCIATION

Mr. RHEEL. Thank you, Mr. Chairman, and Members of the committee, for the opportunity to present Fireman's Fund testimony on behalf of the American Insurance Association on H.R. 4585. It is my privilege to appear before the committee, and I hope that my testimony will provide you with helpful information as you move forward with this bill.

I sit before you today not as an attorney or a regular member or an individual who comes through this great Capitol of ours to testify on behalf of bills. In fact, this is the first time that I have physically been in the Capitol and look forward to future visits.

Instead, my profession and my trade is as a business leader serving the needs of consumers. I would like to share with you today our perceptions of what this bill means to the services we provide to consumers with respect to Workers' Compensation insurance. We all agree that medical privacy is an important issue for consumers and for those financial institutions that hold that information. However, I urge you to take due consideration of the unintentional harm to consumers and other groups that you are seeking to protect. It is our belief that the broad sweeping changes could have negative impacts to consumers and other groups with respect to Worker's Compensation.

In particular, if we look at the basic objectives of Workers' Compensation, which is to provide no fault benefits to injured employ-

ees, a safe workplace, return injured employees back to a productive work life, we believe this bill will prevent us from serving those needs. Preventing legitimate sharing of information with employees and medical vendors and affiliates will prevent us from establishing appropriate timely payments to injured employees, who could not establish with the employer the appropriate work condition to return the injured employee, who could not assist doctors who are not trained in occupational medicine to address medical injuries as it relates to occupational injuries and how to return injured employee back to work, who could not conduct appropriate Work Comp research. Workers' Compensation research is an important element of what we participate in in order to improve the system for all. We also believe we cannot prevent the cost to consumers to increase from litigation, from fraud, from excess litigation as it relates to medical information, and also the cost of adjusted claims would go up with respect to the undue burden of collecting additional paperwork.

Finally, to the consumer, we could not provide the consumers with information on the cost for insurance. As for their fiduciary responsibility to pay premiums as relates to compensation, we could not provide them backup information with respect to that premium. Nearly 50 percent of the cost of insurance for Workers' Compensation relates to medical payments. Not being able to share this information with employers would not give them an opportunity to understand their true costs.

Again, we thank you for the opportunity to testify today, and I would welcome any questions you may have.

[The prepared statement of Robert H. Rheel can be found on page 163 in the appendix.]

Chairman LEACH. Thank you very much.

Mr. Yingling.

STATEMENT OF EDWARD L. YINGLING, DEPUTY EXECUTIVE VICE PRESIDENT, AMERICAN BANKERS ASSOCIATION

Mr. YINGLING. Mr. Chairman, thank you for holding this hearing on medical privacy. Throughout its history the banking industry has protected the medical information of its customers. Our approach is straightforward. Medical information should only be used for the purpose for which it is provided and should not be shared without the express consent of the customer.

Although limited, there are instances where medical information is relevant. For example, in small businesses where the franchise value of the firm hinges on one or two individuals, insurance on these individuals might be required for a loan. In these cases, the borrower will know what information is required and consent to its acquisition and use. Otherwise, medical information should not be used.

On June 6, the ABA, joined by the Financial Services Roundtable and the Consumer Bankers Association, announced new voluntary guidelines on the appropriate use and protection of information. One of the most important guidelines relates to medical information. This guideline states, and I quote: "Medical information will not be shared. Financial institutions recognize that when consumers provide medical information for a specific purpose they do

not wish it to be used for other purposes, such as for marketing or in making a credit decision. If a customer provides personal medical information to a financial institution, the financial institution will not disclose the information unless authorized by the customer."

This and the other nine guidelines represent core values for our industry. Last year, the ABA supported provisions on medical privacy that were contained in early versions of the Gramm-Leach-Bliley Act. We were disappointed that this issue was not dealt with in that legislation. Therefore, the ABA supports the thrust behind H.R. 4585.

The ABA, however, has concerns in two areas. The first relates to process. While broad consensus may be possible on a targeted bill on medical information, the financial services industry would be strongly opposed to opening up the privacy provisions of Gramm-Leach-Bliley on a broader front. The provisions of Gramm-Leach-Bliley need an opportunity to work. The implementing regulations are complex, and I would add that the cost of compliance will be huge. Indeed, for your information, we believe that it is a conservative estimate that the initial cost across all financial services firms will be in excess of $1 billion, with additional costs each year.

The second concern relates to some specific provisions in the bill, particularly the subsection on consumer access to information. We find this provision, frankly, totally unworkable in the real world. We recognize it was taken in large part from the Administration's bill. Under the literal language of the bill, an individual—and that individual does not even have to be a current customer—can demand to see any medical information that might be anywhere in the financial institution, no matter for what purpose it is held. To comply with such a request, the institution would have to ask employees throughout the institution if they somehow had obtained medical information about that consumer. While this may not have been the intent, it is a plain reading of the language.

Perhaps there is a misconception the financial institutions maintain one master list containing all information about a consumer. This is not the case, even for small banks. Typically, there are many lists developed under different circumstances or for different purposes. Moreover, information may be kept in individual employee's files, and never put on any list or on any database. For example, under the bill, a bank would have to go through every check written by a consumer and every credit card slip to see if they couldn't find any medical information, a process that is not done today and a process that is antithetical to the notion of medical privacy.

In conclusion, Mr. Chairman, the ABA believes that medical information should only be used for the purpose for which it is provided. However, the ABA does have concerns about the legislative process going beyond medical privacy and about specific provisions of the bill. We hope that these concerns can be addressed by the committee, and we look forward to working with the committee to that end.

[The prepared statement of Edward L. Yingling can be found on page 171 in the appendix.]

Chairman LEACH. Thank you very much.
Ms. Meyer.

STATEMENT OF MS. ROBBIE MEYER, SENIOR COUNSEL, AMERICAN COUNCIL OF LIFE INSURERS

Ms. MEYER. My name is Robbie Meyer, and I represent the American Council of Life Insurers, the ACLI. The ACLI thanks you, Mr. Chairman, for giving us the opportunity to testify before you today in connection with the Medical Financial Privacy Protection Act, H.R. 4585. We also commend you for calling this hearing and for sponsoring this legislation.

Life, disability income and long-term care insurers are well aware of the very unique position and the very unique responsibility they have regarding an individual's personal medical and financial information. Toward this end, the ACLI board of directors has adopted policy in relation to the confidentiality of both medical information and financial information.

Our policy principles acknowledge the changing horizon of the financial marketplace. We support strict protections for medical record confidentiality. We support a prohibition on an insurer sharing medical records with a financial company such as a bank for determining eligibility for a loan or credit even if the bank and the insurer are affiliates. We also support a prohibition on the sharing of medical information for marketing purposes.

Before I get into the balance of my prepared comments, however, I did want to respond to Congressman Ackerman's statement regarding our sharing of information for posting on the internet, and wanted to state unequivocally that it is a fiction to say that life insurance companies or any ACLI member companies share medical information, encrypted or otherwise, to be posted on the internet in order to decline applicants for insurance or to cause them to be declined for insurance.

The very nature of life, disability income and long-term care insurance involves very personal and very confidential relationships. However, in order for us to serve our existing and our prospective customers, it is essential for us to be able to obtain and use consumers' personal, medical, as well as their financial information in order to perform very legitimate, essential insurance business functions. In other words, life, disability income and long-term care insurers must be able to use medical information as well as personal financial information in order to underwrite prospective customers' applications for coverage, in order to process their claims, and in order to perform essential, and related administrative functions in connection with those contracts.

It is essential for us to share and disclose information in order to fulfill legal and regulatory mandates. In other words, it is essential for us to disclose confidential medical information to State guaranty funds. They need to be able to have access to individual identifiable health information in order to evaluate health information claims that a claimant might submit in connection with an insurance company that has become insolvent. Insurance companies also need to make disclosures and to share information with State insurance departments and law enforcement agencies in order to detect and deter fraud. Also, in connection with very ordinary basic

business transactions such as reinsurance treaties or mergers and acquisitions, it is also necessary for us to share our customers' information in order to effectuate those business arrangements.

As you know, Title V of the Gramm-Leach-Bliley Act enacted the strictest regulatory framework ever enacted into law in connection with financial records privacy. We very much appreciate the fact that your bill, Mr. Chairman, tracks the general framework of Title V in seeking to balance consumers' very legitimate and grave concerns about their confidentiality rights with insurers need to use consumers' medical, as well as their financial, information in order to perform legitimate insurance business functions which are necessary for us to meet American consumers' insurance needs. However, we are concerned that the bill fails to achieve this balance, primarily because of its failure to totally track the Gramm-Leach-Bliley framework. In other words, we are concerned that the bill does not include the Gramm-Leach-Bliley provisions dealing with the necessary sharing of information by a financial institution with the State guaranty associations.

We are also worried about the fact that it does not include the provisions permitting financial institutions to share information with service providers. That concern arises because many of our member companies have independent agents who are not company employees, with whom they would now have difficulty or be hindered in having ordinary business communications about proposed new insurance policies, or the best policies for a particular individual under particular circumstances.

We are also concerned by the broad rights the bill grants consumers to access and correct information held by a financial institution, primarily because the bill does not clearly protect from that access information that an insurer may have collected in connection with a fraud or a material misrepresentation investigation and also materials collected in preparation for litigation.

Finally, the ACLI strongly supports the concepts of a Federal preemption. We feel very strongly that individuals who live across the country should not have to be concerned that they have different medical records privacy protections depending upon the State in which they live.

And, finally, we would like to thank you once again, Mr. Chairman, for giving us the opportunity to testify.

[The prepared statement of Robbie Meyer can be found on page 182 in the appendix.]

Chairman LEACH. Thank you all very much. Your testimony is very helpful and certainly as we go forward suggestions of a specific legislative nature we will certainly review as well.

Mrs. Roukema.

Mrs. ROUKEMA. Thank you, Mr. Chairman. I am not sure that I heard with specificity the explanations as to how people or how individual groups stood on the subject of the mental health disclosure question. But I will say, putting it another way to this group, as I have on other occasions to business groups, there are certain issues that are becoming highly emotional and highly political that have the potential of creating a backlash. And I think you are all aware of this, particularly if you have been reading the press lately or you have been reading our e-mails lately, the potential of cre-

ating a backlash—and you saw some of that when we got into the controversy here on the committee with H.R. 10 and in conference on H.R. 10. We had to pull back from some of the things.

But the point is that if we can't come up with a precise definition in this brave new world of instant communication, and also these new holding companies and affiliate relationships, if we don't come to terms with that, and get thinking minds on both sides of the issue, whether it is the health care professionals or the insurance groups or the physician services together, we may end up with something that all of us are going to wring our hands over. And so I didn't hear everyone's comments, but I do have to ask my good friend and former colleague, Mr. Bartlett, I am sorry that I really didn't hear any specific reason as to where your group or any of the other groups might object to the mental health provision. It seems to be blatantly obvious out there. And I don't know what is so objectionable to treating that as a separate entity, as the Chairman's bill proposes. Mr. Bartlett, if you want to substantiate some of your general comments or if anybody else wants to add to it, please.

Mr. BARTLETT. Madam Chairwoman, we are available to be convinced. Essentially we look at this bill not as an opt-in bill or not as an affirmative consent bill. We look at this bill as a prohibition against using medical information other than for purposes for which it was intended. We think that same prohibition ought to apply to mental health information or physical health information. And I took a very careful look at this, because it is a new approach and it is an approach that is talked about and I knew it would be a hot one. We couldn't identify any benefit to having a separate consent for mental health from physical health. We think that it is a prohibition against the use of information. Ought to stay that way. And we couldn't see a benefit to adding a second or a double consent procedure, just didn't—other than adding paperwork and consumer confusion, we couldn't find anything that someone would want to consent on for mental health information that they wouldn't consent with for physical health information.

We could be convinced. We couldn't find any reason to do it.

Mrs. ROUKEMA. We are going to have to convince you, I think. But no, I think the woman on the previous panel—I am sorry, her name escapes me right at the moment, but in answer to my question did say that the insurance group didn't have an official position, but in her own opinion she thought there was a reason for a separating.

Dr. Harding, do you want to comment. I am sorry, I am talking about Kathleen Sebelius, the Insurance Commissioner in Kansas. Mr. Harding, do you want to amplify on your own position in response to what has been stated on this panel?

Mr. HARDING. Yes, ma'am. Only that in an ideal world allergies and psychosis would be handled the same. That certainly would be the goal of all of us. But in the real world, because of prejudices or stigma or whatever you call it, certain illnesses have a higher sensitivity than others, and until we overcome that societal prejudice or stigma we are going to have to look out for special circumstances within the medical field that needs special sensitivity

protections. But hopefully someday we will have that where it will all be the same.

Mrs. ROUKEMA. Thank you. I appreciate that. I just hold out the hand of cooperation here, because again I want to avoid a kind of backlash that is going to force us into some very untenable positions in the near future. And we have—it is no secret that there is an election coming up and there are all kinds of ideological or demagogic positions that can be stated on these highly sensitive issues, and I would like to work with everyone on this and come to an intelligent and reasoned conclusion.

Thank you.

Thank you, Mr. Chairman.

Chairman LEACH. Thank you, Marge.

Mr. Ackerman, do you have any questions?

Mr. ACKERMAN. Yes, thank you, Mr. Chairman. I am sorry I was out of the room. I am at two hearings at the same time, but I understand that Ms. Meyer made reference to the question that I raised with the first panel. And if I am not mistaken, what I have been advised is you categorically denied that any such system exists whatsoever whereby the insurance companies, some insurance companies, at least one insurance company does not reveal to a prospective person who has had their medical exam what the results of that exam is, if it is a medical claim, that they have paid for the exam and therefore it is not the property of the consumer, turns the person down for insurance, and then posts on the computer for all agents to know not to rewrite the policy of that person because he tested positive for AIDS and the person does not know that. In this particular case, the person died.

Ms. MEYER. If that happened, that would be absolutely positively contrary to ACLI policy and that of our member companies.

Mr. ACKERMAN. In that case would you reverse your policy and support the legislation I tried to introduce that would prevent that from happening?

Ms. MEYER. I am sorry, I am not familiar with your legislation, but we would be delighted to take a look at it.

Mr. ACKERMAN. It will be my intent, Mr. Chairman, to offer hopefully a friendly and humane amendment that would say that if an insurance company, albeit their physician who pays for the cost of a person's exam and that person is turned down, that that person is entitled to know why he was turned down.

Ms. MEYER. We absolutely agree that if someone is declined for insurance coverage that they are entitled to know the reason why. A requirement to get that information actually is in the law in the sixteen or eighteen States that have enacted the old NAIC model on privacy. The ACLI has supported that model for decades.

Mr. ACKERMAN. The reason for declining support was given as it would be too expensive to notify all these people about their illnesses that caused them to be turned down for insurance, albeit this one was certainly a life threatening and life taking incident. So you are saying that you would be supportive?

Ms. MEYER. I, as an attorney, would have to look at the words, but we are absolutely strongly in support of an individual being informed of the reasons for any adverse underwriting action taken by an insurer.

Mr. ACKERMAN. Would you be willing to cooperate with us in our determination as to whether or not it was posted on the computer system that this particular person, when his existing insurance was up, should not be rewritten if he was late in payment?

Ms. MEYER. This sounds like a fascinating case. A life insurance policy, once it has been issued, cannot be canceled for any reason except for nonpayment of insurance claims. The only thing that can happen with the life insurance policy is that premiums can actually be decreased if an individual becomes more healthy after they have had a policy in effect.

Mr. ACKERMAN. The inference here is that it was posted so that if this person's premium was due on the 4th and it arrived on the 5th, he was to have his insurance declined for late payment and should not be extended the courtesy because of specific reasons.

Ms. MEYER. We would be delighted to sit down and see what has happened here. This sounds like a horrible situation.

Mr. ACKERMAN. It is, when we get to computers and people's private information and who has control of it. And I thank the Chairman for allowing this line of questions.

Chairman LEACH. Thank you, Gary.

Well, let me thank the panel. And we appreciate very much their testimony. We hope to work with them.

Oh, excuse me. Mrs. Biggert. I keep overlooking you. I am very, very sorry. I apologize.

Mrs. BIGGERT. Thank you. I am still here. At least I am not at the kiddie table, so I am in the front row. I do have a couple of questions if I might.

Chairman LEACH. Please, and feel free to take extra time.

Mrs. BIGGERT. Thank you.

Mr. Rheel, based on your professional experience in the insurance business, do you know of any instances of abuse by the insurance companies or their business partners of any access to health information at the current time?

Mr. RHEEL. I am unaware of any abuses as it relates to information held by insurance companies. And we take very seriously the information that we have in our records and do not freely release the information for any unrelated transaction or for a need of the information to any third party.

Mrs. BIGGERT. Can you tell me what the practice of and when would insurance companies require health information when considering an application for insurance?

Mr. RHEEL. From a property and casualty standpoint, medical information that we seek is generally aggregate information. It does not pertain to an individual employee or to the consumer. We make decisions based on information on the aggregate levels from a property and casualty standpoint. That is my field of expertise in that area. Our underwriting is based on risk conditions, not employee conditions as it relates to the individual employee or to the consumers themselves.

Chairman LEACH. Excuse me, Mr. Rheel, if you could pull the microphone a little closer we would appreciate it.

Mrs. BIGGERT. I think I am through with the witness. But if I could ask Dr. Harding, are doctors and psychiatrists required by

law to protect patients' medical records? So how do these records get transferred to the third party, such as an insurance company?

Mr. HARDING. Well, insurance companies often ask for details of medical care as part of the payment for those cares. There is a third party involved between a physician and a patient and an insurance company. So they ask for varying amounts of information from the physician with the consent of the patient for means of payment. So they then receive from me in my case information, the smallest amount that I can get away with giving them actually, information that they will then use to determine if the treatment was appropriate and whether they should pay the amount of money that I ask them to. That is how they obtain it originally, although in a hospital setting it is a little different, but there it is usually with the consent of the patient that it goes to the insurance company.

Mrs. BIGGERT. So really if someone had no insurance, then there probably would be not any or, for example, a bank that would not have access to any?

Mr. HARDING. Oh, but I think that is where we start getting into some interesting areas because, for instance, if a patient came in to see me and paid cash, didn't have insurance, and I gave them a prescription, they went down to their local pharmacy, handed in the prescription and paid that prescription with a Visa card, all of a sudden the record of what they bought would be in the financial system. Now, it doesn't take a rocket scientist to know that if that prescription is for Prozac that might be a psychotropic medication that many people are aware of and that would start a process that potentially has concerns for that patient's medical privacy, and which was not intended by any means, but it is part of the financial system.

Mrs. BIGGERT. Mr. Bartlett, you look like you might want to say something.

Mr. BARTLETT. Technically or potentially, as I said in my testimony, potentially that could be true, but in reality it is not. No financial institutions collect such sort of information. We believe they are prohibited by all manner of laws, court cases and regulations from collecting it. No financial institutions uses such information or even collects it. So while this is good legislation to close a potential loophole, I do want the record to reflect that such a situation so far as I can tell doesn't happen, it is not likely to happen, and this legislation would help to prohibit such a thing from happening, but it doesn't happen today, and wouldn't happen in the future, I don't believe.

Mrs. BIGGERT. OK. And you also said in your testimony that the issue of including an exception for sharing medical information to permit joint marketing of products—what is a joint marketing of products?

Mr. BARTLETT. I added several exceptions and my exceptions tracked Gramm-Leach-Bliley, which had quite good exceptions. The most important exception was for rating and State guaranty funds, as has been testified here. We think that is absolutely essential. Otherwise you just abolish the whole system of rating tools.

In terms of joint marketing, again that was in Gramm-Leach-Bliley. We think that there are particularly service providers, agents,

independent agents that need to have information as an extension of the company, and that is again using the medical information for the purposes for which it was intended, not for any other purposes. So we would encourage the committee for the purposes of the exceptions to track Gramm-Leach-Bliley and then the prohibitions is an additional and much stronger set of prohibitions of the use of the information. But the exceptions should track Gramm-Leach-Bliley.

Mrs. BIGGERT. And then just a general question, we have been looking at this privacy issue and protecting patient's medical records, and this was put on to the Gramm-Leach-Bliley bill, but should we really take a look at this just as comprehensive legislation on the subject rather than just legislation dealing only with financial institutions?

Mr. RHEEL. One of the issues facing this committee is the complexity of products of financial institutions in a new brave world—as we have been talking this morning about—is that there are many products. The impact of medical information has different issues with different products. We talked about life insurance, and my field of expertise is Workers' Compensation. The impact of medical information is critical to Workers' Compensation providing the service to the consumer.

So I would urge this committee to look at the various components of the financial institution and address the issues that you are concerned about specifically, not broadly over the entire financial institution. We talked a little bit about the rating organizations, the need for information for them to create rates, research organizations needing information to conduct research to improve the system. So there is a particular need for every product and the use of financial information, who uses it, and the purpose of that information changes product by product.

Mrs. BIGGERT. So you would agree with what was maybe suggested in one of the earlier panels that we should look at Workers' Compensation as perhaps an exception to this because of the opt-in provision?

Mr. RHEEL. Yes, I would.

Mrs. BIGGERT. Opt-out provision.

Mr. RHEEL. I would encourage the committee to consider exceptions like Workers' Compensation because of those needs. What we deal with in the property casualty world is the third parties, and third party actions. They are making their medical condition an issue. It is an issue that they are bringing claims to consumers and looking to their financial institutions, in this case insurance companies, to protect. In order for us to do our responsibility to protect those consumers, we need that information. As a standard practice, we provide that information to medical vendors who provide expertise back to the process to ensure that we are providing the best care to injured employees and also the best services to our consumers.

Mrs. BIGGERT. Thank you.

Thank you, Mr. Chairman, for your indulgence.

Chairman LEACH. Well, thank you very much, Mrs. Biggert.

I would like to thank the panel. In particular, I want to thank Professor Harding. The reason I say this is you come to this table

with some limitations on free speech that the rest do not have. And you might wonder why I say that. A couple of decades ago the officers of your association visited me, advocating or opposing some bill on Capitol Hill, I forget what it was, and I uttered the opinion that I thought a former high ranking public official, in fact a President, had exhibited certain signs of what I would describe as paranoia. I asked them if they agreed with me. And they looked at each other and the president of your association then responded, "Well, it is this way, Congressman, it is inappropriate for a psychiatrist to comment on someone he hasn't examined, and if he has examined them, it is inappropriate for him to comment without the person's permission. And in any regard, our licenses would be lifted if we said something exhibiting a psychiatric judgment about a public official."

So it strikes me you have first amendment constraints that no one else in the country has. So I am particularly appreciative of your coming, but I maintain the view that this particular President was crazy.

Mr. HARDING. I won't ask you which one.

Chairman LEACH. But I can say that as a non-trained, non-subtle, non-informed individual. Anyway, thank you all.

Our next panel, we have Nicole Beason, Esther Peterson Fellow at the Consumers Union; A.G. Breitenstein, who is Chief Privacy Officer of ChoosingHealth.com; Evan Hendricks, Editor and Publisher of Privacy Times; Mr. Edmund Mierzwinski, who is Consumer Program Director of the United States Public Interest Research Group; Joy L. Pritts, who is Senior Counsel, Health Privacy Group of Georgetown University; and Mr. Ronald Weich, who is an Attorney with Zuckerman, Spaeder, Goldstein, Taylor and Kolker, LLP, on behalf of the American Civil Liberties Union.

And we will begin with you, Ms. Beason.

STATEMENT OF NICOLE BEASON, ESTHER PETERSON FELLOW, WASHINGTON OFFICE, CONSUMERS UNION

Ms. BEASON. Mr. Chairman——

Chairman LEACH. Excuse me, if I could ask, if you pull the microphone quite close I think it is a little easier.

Ms. BEASON. Is this good?

Chairman LEACH. Yes.

Ms. BEASON. Mr. Chairman, Congressman LaFalce, Members of the committee, my name is Nicole Beason, and I am the Esther Peterson Fellow at Consumers Union. As you may know, Consumers Union is a nonprofit publisher of *Consumer Reports*, and we are here today because we believe that protecting the consumer's medical privacy is a very important issue. What is at stake here? Strangers knowing that at a young age you had a hernia, as a teenager you developed asthma and now as an adult you recently had bypass surgery. You should be able to have your health checked and treated without having your privacy violated.

Consumers Union has identified certain privacy principles that we believe should be included in any legislation intended to protect consumer privacy. First, every consumer has a privacy interest in individually identifiable health information.

Second, waivers of an individual's privacy interest should be made clearly and conspicuously and limited to scope to specific purposes. In fact, we have consistently advocated for an opt-in approach to the release of personal medical or physician information. Opt-in simply means that the institution must get the consumer's permission before sharing information about that consumer.

Third, financial institutions, health care providers and other holders of health information have a duty to maintain the confidentiality of personal health information and should be held accountable for protecting an individual's privacy interest. Personal health information provided to a financial institution by a consumer should not be transmitted to anyone else, including affiliates and third parties, without the consumer's clear awareness and consent.

Consumers should generally have the right to access and ensure the accuracy of their own health information. Consumers should also have the ability to amend and correct inaccurate information. Inaccurate information could have serious consequences should a consumer consent to sharing their health information. For example, they could be denied health coverage because their records falsely indicate that they have a poor medical history. Therefore, a mechanism needs to be implemented to ensure that consumers will be able to amend and or correct their information.

They also need to be given notice when and a reason for why such requests for amendment and correction are denied by the financial institution. It is also important that consumers are given the identity and referred to the original creator of the inaccurate information. The Fair Credit Reporting Act can serve as a model for the regulators to use to implement this requirement.

Specifically, we are concerned that one of the parties who has a vested interest in this information is not allowed to make a blanket determination as to whether the disputed information is included or shared with other parties. The financial institution or the generator of this information should not automatically deny a consumer's request to amend and correct medical information. Therefore, a dispute process like the one used under FCRA should be adopted.

Because H.R. 4585 addresses these issues, Consumers Union supports Chairman Leach's legislation, with some suggestions to strengthen this bill. The concerns about H.R. 4585 that we share with other consumer advocates, the extensions, if any, should be limited. The bill should not contain any loopholes that would allow financial institutions to share consumers' medical information counter to the intent of this bill. A financial institution should not be allowed to use health information about a consumer without the consumer's consent, not just for decisions regarding the loan or credit for any product or service offered by the institution to the consumer.

While it is important to focus on medical privacy, there are other components of privacy that consumers care about. We urge this committee to not just take up this narrow aspect, but to look at a broader privacy package.

Mr. Chairman, once again thank you for the opportunity to testify before the committee today. I would be happy to answer any questions the committee may have.

[The prepared statement of Nicole Beason can be found on page 196 in the appendix.]

Chairman LEACH. Well, thank you very much, Ms. Beason.

Ms. A.G. Breitenstein.

STATEMENT OF A.G. BREITENSTEIN, JD, MPH, CHIEF PRIVACY OFFICER, CHOOSING.HEALTH.COM

Ms. BREITENSTEIN. Chairman Leach, Representative LaFalce, thank you for inviting me here today. My name is A.G. Breitenstein. I am one of the first Chief Privacy Officers of an internet startup. ChoosingHealth.com is the service which allows patients to communicate with each other and with their providers and hospitals and researchers without having to give up their privacy. We are dedicated to the notion that people's information belongs to them, and I want to take this time to thank you for taking up this issue.

A *Wall Street Journal* poll recently found that Americans consider the issue of health privacy to be more threatening than domestic terrorism. A Harris poll has also found that privacy is the number one reason that Americans are staying off the internet.

The urgency of this problem is very, very clear. Nancy Dickey, the past President of AMA, has stated the following, "These days insurance companies don't want summaries, they want the whole record. So I think twice about what I include, and then I hope I can remember it all. If my patients fear that what they tell me could come back to haunt them, they tend to be less forthright. I may come up with the wrong treatment, because I was chasing the wrong clues."

And Nancy Dickey is not alone. I myself counseled a doctor whose wife was an OB/GYN and he told me that his wife routinely doodled in the margins of her record. The reason was that she used these doodles to code messages to herself about her patient's medical histories. She felt that this was important to do to protect the privacy of her patient's records, but feared that if anything ever happened to her, her patient's records would be impossible to read.

I also want to read you a quick quote from a pediatrician I worked with. He said to me, "Insurance companies are requesting as part of well visits to ask and document, which I have no problem with, children questions, such as "Do you have sex?" "Do you masturbate?" "How are your relationships with your parents and friends?" "Have you had an abortion?" And many others. As I said, I have no problem with asking these questions. What disturbs me is the access that insurance companies have to that information and therefore anybody else that wants or can legally obtain those records. We physicians are in a Catch-22. If we document, patient confidentiality can be destroyed. If we don't document, we are classified as bad physicians. As a pediatrician, I am very concerned about how this information available to third parties will affect these children's futures."

Basically patients are put in a position of having to make a choice between their health and their privacy. I want to support you in this legislation. This legislation is a very good first step. If there is one thought that I can leave you with in terms of my testimony, it is this: Personal information, particularly health informa-

tion, is the new cash in this digital age. Your efforts to protect privacy of personal health information will set the terms that allow patients to negotiate on a level playing field for the value of this new currency. Without adequate protections individuals will be robbed of a valuable resource and will be reluctant to purchase the goods and services they need on the internet.

What do I mean by this? People get "free" stuff, and I put free in quotes, in our new digital economy, because they are willing to give up certain aspects of personal information in exchange for this. This is very true on the internet. Most websites have as their primary revenue model some plan to sell this personal information collected, and personal health information is the most valuable of all these categories of information.

If I, as a bank, can collect and sell a list of people who have asthma to unscrupulous researcher or a direct marketer, I can make millions of dollars.

How should this affect your work on H.R. 4585? Privacy legislation will be the backdrop against which the emerging digital economy will be set. It will have a profound influence on the ability and right of consumers to negotiate the value of their personal information in exchange for goods and services. You are in effect creating a new currency of sorts.

There are a few suggestions I would like to make to this end. The basic rule of consent must be clear and unambiguous with few exceptions, and this consent should be voluntary. Health information collected for one purpose cannot be used for another purpose without consent. I was particularly troubled by the exception for joint marketing that is in the legislation now. It seems to me that this is a loophole for sort of reconfiguring the marketing schemes that people are protesting and as long as it is done along with the entity that first collected the information, this seems like a very large loophole. There are also——

Mr. LAFALCE. Excuse me. Where is that last concern expressed in your testimony? I was following you on point two and I didn't follow you when you were underscoring a point.

Ms. BREITENSTEIN. It is not in my written testimony, but I would be happy to amend it for your purposes.

Mr. LAFALCE. Please do so.

Ms. BREITENSTEIN. As the banking insurance functions begin to merge under this Act, it is going to be exceedingly——

Chairman LEACH. For point of clarification, the concern you have in joint marketing is not in the bill. It is advocating——

Ms. BREITENSTEIN. In the original, correct.

Chairman LEACH. But not in H.R. 4585?

Ms. BREITENSTEIN. Correct, it is in the exceptions that are referred to in H.R. 4585.

Chairman LEACH. So this is a concern about an advocacy of position that another panelist has suggested, but not a concern about the bill itself, is that correct?

Ms. BREITENSTEIN. Correct. It is a concern for pulling those exceptions into this bill. Does that make sense?

Chairman LEACH. Sure.

Ms. BREITENSTEIN. Great.

As banking and information functions begin to merge, it is going to be exceedingly important to make sure that the firewall between these areas is enforced.

Finally, individuals must have a right of action to enforce their claims on their own personal health information. Data is property. And if there is one thing we have historically protected in this country, it is the right of an individual to protect their property. Failure to do so will not only adversely affect health care, but will set a dangerous new precedent in this information era.

Many of my esteemed colleagues have testified today that these protections are going to drive up costs and stymie economic growth. I want to challenge this argument head on. Personal information is a resource. It has value as our economy shifts to an information based system. It will become one of the most valuable resources in the world. If we rob individuals of their data, we will render them penniless and powerless to participate freely and fairly in this new market. We will first feel this in rising health care costs, owing to an eroded doctor-patient relationship. We will then feel the effects of when people offer erroneous information or choose not to participate at all.

I want to thank you and offer any suggestions I can for improving this.

[The prepared statement of A.G. Breitenstein can be found on page 202 in the appendix.]

Chairman LEACH. Thank you very much, Doctor.

Mr. Hendricks.

STATEMENT OF EVAN HENDRICKS, EDITOR AND PUBLISHER, "PRIVACY TIMES"

Mr. HENDRICKS. Thank you, Mr. Chairman. I am Evan Hendricks, editor and publisher of *Privacy Times*. I have been reporting on and following privacy developments in Washington since I arrived here in 1977. I am in my twentieth year of publishing *Privacy Times*. There is always a tendency to take good news for granted, and I don't want to do that. I think the good news here is you, Mr. Chairman, and the Ranking Minority Member. You have always been willing to give privacy a fair hearing. You are the first one to tackle the tough information of information brokers. With the help of Mr. LaFalce, the two of you have taken a bipartisan approach to privacy and I have seen the benefits for Americans in that, and I am glad to see that continuing today.

I think the bad news is that there is not another committee Chairman that followed the example that you set. I hope that that will be changing as it becomes clearer to Washington how important privacy is to the American people.

I think what we have in front of us today is a good bill. The core of this bill is good, because it is based on affirmative, informed consent, which should be the baseline of all privacy law and information usage in the United States. And I think it is only a matter of years before we get that kind of privacy law and information usage in the United States. So I of course advocate speeding the way there.

Of course, no bill can be perfect. They can all be improved, including the Administration's and including the one before us today.

And so I incorporate the comments of my fellow panelists, ACLU, Dr. Breitenstein, Consumers Union, for some of the specifics I would like to speak to. Traditionally in the United States we have always taken a narrow approach on privacy. Certain issues come up, like we found in Judge Bork's situation where a newspaper reporter got ahold of his video rental records, and this was an issue that hit close to home in Congress and they moved quickly to pass the Video Rental Protection Act. But the narrow approach has left us with many of these gaps.

So we do have the Fair Credit Reporting Act, an important law that this committee had a role in, video rental records are protected, cable TV is protected. But many important types of records like medical records, employment, some kinds of financial information, internet, retail records are not protected. And this is extremely significant that now in history we are in an age of convergence, where we see under Gramm-Leach-Bliley the convergence of insurance and banks. We see the convergence of means of communications. The internet, cable, telephones, the banking and the wireless system are all converging. I think we really need to move toward a comprehensive approach to privacy if we are going to have our laws fit the technology and the information systems that we have. And so I favor in just the area of financial privacy the starting point for considering financial privacy would be the Administration bill as introduced by Congressman LaFalce. That would take a more comprehensive approach to the issue of financial privacy, and I think that is where we start.

I think it is also important to point out, though, that there is rampant public concern now about privacy. Even in our newsletter we have reported bits and pieces about some of the politicians' proprietary opinion polls showing that privacy is off the charts among Americans, and the *New York Times* fleshed this out a week ago Sunday in the Week in Review section, showing both Republican and Democratic polsters are finding that this is the sleeper issue of this campaign.

The lesson learned, we must do something dramatic and comprehensive to respond to the well-founded public concerns about privacy and I think the solution is that the Administration really has a responsibility to come forward with a comprehensive national package. If the Administration doesn't do it, then the leadership of the Congress should do it, although traditionally this role has belonged to the Administration.

Now, I think one reason the Administration hasn't done this is for too long the Commerce Department has been at the middle of the Administration's privacy policy and for too long the Commerce Department has been kneeling at the altar of voluntary self-regulation, and still does, well after voluntary regulation has been discredited as feasible or workable. I think the Commerce Department should get out of the privacy policy business altogether and just go back to counting beans.

The good news, though, is that the Treasury Department has come forward with a comprehensive financial privacy bill. The Federal Trade Commission has now recommended national privacy legislation for internet privacy and Health and Human Services is moving on medical privacy, telling Congress they need to go beyond

what HHS can do in rulemaking. So we have, through fits and starts, we have the pieces of what could be a comprehensive privacy policy.

I think on top of this we need privacy infrastructure. No matter what happens, we are still going to have to integrate and consolidate and rationalize privacy laws so they are consistent across mediums and for kinds of records and have reasonable differences for reasonable context so there is consistency. And this is the role of what other countries, all of the Western countries have, and we don't, and that is a privacy commissioner, an independent privacy commissioner that would offer answers to the legislature. That is a very important step in creating the privacy infrastructure we are going to need to have a rational scheme of privacy protection.

Finally, I think it is important to note that one of the most pro-consumer developments is the development of the internet and e-commerce. Yesterday Chairman Pitofsky of the FTC was talking about the benefits to consumers. There is a real risk, and we are seeing the numbers, and that the phrase "burn rate" is a very dominant phrase now that the "e-tailers" are going to go out of business. That is partly because we have not created an environment of consumer confidence. Without adequate privacy protection, we will not have consumer confidence. Not only is this the best thing for the American people and something that will eventually happen, but something that is absolutely necessary for us to make e-commerce flourish. Otherwise it is still possible we could have the unfortunate debate of "Who lost e-commerce?"

Thank you, Mr. Chairman.

[The prepared statement of Evan Hendricks can be found on page 207 in the appendix.]

Chairman LEACH. Thank you, Mr. Hendricks.

I am also struck by the fact that you had a magazine that has been in existence for twenty years, and privacy as a concern didn't emerge until six months ago. Thank you.

Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP

Mr. MIERZWINSKI. Thank you, Mr. Chairman, Mr. LaFalce. I am pleased to offer the views of the U.S. Public Interest Group on your important new legislation to protect consumers' financial medical privacy. We want to commend you for introducing a bill that is very supportable, with some amendments, and we are encouraged by the fact that the core of your bill recognizes that opt-in express consent by consumers should be the criterion upon which information is shared or used for secondary purposes. As Mr. Hendricks has articulated, we believe that any privacy laws should be based fundamentally on opt-in consumer consent.

We are especially pleased that a number of parts of your bill are quite strong, particularly its provision that the use of information already held by an entity requires express consent and also its stronger provisions in the areas of mental health.

That being said, I do have a few points in my written statement on areas where we think that the bill could be improved. We also

think that some of these areas apply equally to the President's bill. And let me just discuss those very, very briefly.

First, I think both bills have too many exceptions and that the committee ought to look very carefully at the need for those exceptions. I am quite aware that the industry witnesses believe there should be more exceptions, but we believe to protect privacy there should be as few as possible.

Second, in the area of coercion of consent, we are generally concerned that consumers not get into the habit of ignoring warnings and simply giving consent as a condition of applying for any kind of an account. And in this area, the President's bill uses one approach, your bill uses a different approach.

We believe perhaps the best solution might be a combination of the two approaches, with the addition of the approach taken by the comprehensive medical privacy bills, not only the financial privacy bills, but some of the other bills before the Congress that would prohibit the conditioning of any treatment or provision of any service upon provision of consent.

The third area is the issue of loans or credits. The strongest parts of your bill appear to be limited only to the issuance of loans or credit. We believe that this potentially means that banks and financial services holding companies might be able to use confidential health-related information for marketing purposes, for example, or employment purposes, for example, and we would suggest that you eliminate that narrow structure and broaden the definition so that it applies not only to loans and credit, but to all uses of information by a holding company.

Neither bill, your bill nor the President's proposal, provides a private right of action under Title 5. We believe that a fundamental privacy protection is to give consumers the right to sue when their rights are violated.

One area where we think you could come to some congruence with the President is on the important area of access, providing the opportunity for consumers to correct and copy their financial medical records. Your bill, of course, includes this strong provision. The President's bill, however, includes that provision and applies it not only to health records, but also to financial records.

The industry often complains about complex regulations, burdensome complex regulations. How could I forget the adjective "burdensome"? The way you could make the regulation more simple would be to apply the access and correction provisions not only to medical information, but also to all information held by a financial services holding company. To give consumers that Fair Information Practice as it applies to all of their information, we think would be a good step forward. Then instead of being under two regimes, the banks would only be under one regime for complying with that provision of the law.

We believe also that as the bill relates to HIPAA, there is language in the bill describing the relationship between the two bills. We think there should be an expressed provision that says stronger privacy law controls in all circumstances. That would be a notable improvement to the bill.

We are very pleased that both you and the Administration have recognized, as has the broad coalition of consumer, pro-family, free

speech and civil liberties, and privacy organizations that have been supporting privacy legislation in this country, that the core of privacy legislation should be expressed opt-in consent. We would urge you to work together with the Administration.

Your bill applies to medical privacy. The President's bill, as introduced by Mr. LaFalce, applies to an opt-in regime to both medical privacy and sensitive financial information. We would urge, of course, that that be broadened to include all medical and all financial information, and ultimately, as Mr. Hendricks has described, that we establish opt-in financial consent across all areas of the economy, because as the industry groups are converging, as companies that used to do one thing are doing many things, the gaps in our privacy law are becoming clearer and clearer.

That being said, we commend you for introducing a bill to solve the most important loophole in the Gramm-Leach-Bliley Act; and that is, its missing provision on medical financial privacy and we urge support of your bill. Thank you.

[The prepared statement of Edmund Mierzwinski can be found on page 211 in the appendix.]

Chairman LEACH. Thank you.

Ms. Pritts.

STATEMENT OF JOY L. PRITTS, SENIOR COUNSEL, HEALTH PRIVACY GROUP, GEORGETOWN UNIVERSITY

Ms. PRITTS. Good afternoon. I would like to first thank you, Mr. Chairman and Congressman LaFalce, for giving us the opportunity to testify today on this important issue of health privacy.

I am with the Health Privacy Project, which was formed a few years ago. The mission of the Health Privacy Project is to raise public awareness about the importance of ensuring privacy of health information from the standpoint of improving health care access and quality, not just from an individual point of view, but also from the community's point of view. We believe that this is an important area which, as technology changes, is subject to more and more threats.

Given the focus of our project, we follow the privacy components of the Gramm-Leach-Bliley Act with great interest. Financial information often overlaps with health information, and we have had concerns that in the process of modernizing the financial services industry, sensitive health information might be turned into just another marketable commodity, and we don't think it should be that type of information.

The bill that is at issue here today, H.R. 4585, goes a long way toward addressing our concerns with that issue. I would like to address some of the major components of that bill.

One of the first things that we focused on was the opt-in requirement for a financial institution to release the information of a consumer. An opt-in requirement is pretty much the status quo in other Federal bills, and we believe that this is the way to go. We also believe that this is a vast improvement over the opt-out provision that was in the original Gramm-Leach-Bliley Act, because that kind of presumes that a consumer would consent to the release of this information, and we don't think that that presumption is very

accurate, that people would voluntarily release this information if they knew how it was going to be used.

We also appreciate the fact that this opt-in requirement applies to non-affiliates. From a consumer's perspective, it really doesn't matter if the information is going to an affiliate or non-affiliate. The key issue is whether the information is being released from the original record holder.

Another aspect of this bill that we were pleased with is that it addresses consumer profiles. Although we have heard today that banks do not use medical information in this manner, I think it is quite obvious from anybody who has received a statement of a checking account, that many of us at the end of the year receive a statement that lists how things have been processed. Your credit card statement says how your money has been spent during the year and it includes things like a category, $10,000 for health information during the last year.

So the technology is there and it is something that in the future people could possibly do.

One other area that this proposal addresses is that it restricts the use of health information for providing certain financial services. We see this as an improvement over the original Gramm-Leach-Bliley Act. There are a lot of consumer concerns that their health information may be used to deny them access to financial services such as loans and credits. There was a question posed earlier today to another panel about whether anybody knew of any circumstances under which that had actually happened. We are aware of an article that was in *Time Magazine*, I believe it was in 1996 or 1997, where they reported an example of a bank officer who also happened to serve on a State board which governed a cancer registry, and the bank officer ran a list of the people who had been reported as having cancer and he used that listing, compared it to the files in his bank, and apparently he terminated their loans. Now, that is really kicking somebody when they are down. So there are circumstances that have been reported where this has actually occurred, and we would really like to see a prohibition on that occurring in the future.

Another major improvement in this Act is a provision that would grant consumers the right of access to and to correct their information. If your health information is going to be used to make life-influencing decisions, such as whether or not you are going to get insurance or you are going to get a mortgage, or if it is going to be spread to other people for them to use, you should certainly have the ability to see what information is out there about you and to correct it if it is inaccurate.

Although we support the opt-in requirements for use and disclosure, we do believe that those requirements mean almost nothing if they are not truly voluntarily signed, and if a financial institution is able to condition the provision of a financial service on a consumer's executing those authorization forms, it is not really voluntary. It is not really an authorization if you have to do it in order to obtain a loan, for instance. This is one area where we really believe that this bill could be improved.

Overall, we are quite happy with the provisions in H.R. 4585 and we are pleased that it has been introduced. We look very much for-

ward to seeing the gaps in the Gramm-Leach-Bliley Act filled, and it looks like we are moving in that direction and we would be happy to assist with that process if we could.

[The prepared statement of Joy L. Pritts can be found on page 214 in the appendix.]

Chairman LEACH. Thank you, Ms. Pritts.

Mr. Weich.

STATEMENT OF RONALD WEICH, PARTNER, ZUCKERMAN, SPAEDER, GOLDSTEIN, TAYLOR AND KOLKER, LLP, ON BEHALF OF THE AMERICAN CIVIL LIBERTIES UNION

Mr. WEICH. Thank you, Mr. Chairman. I appreciate the opportunity to be here today to speak on behalf of the 300,000 members of the American Civil Liberties Union.

As the fourteenth of fourteen witnesses at today's hearing, I think it is my responsibility to say something that nobody else has said, and say it briefly. What I would like to do is first of all endorse the recommendations for strengthening the bill that my colleagues on this panel and that the Treasury Department official on the first panel put forward. But I want to take a step back and remind the Chairman and the Ranking Member of the importance of this legislation for health and public health.

Over the course of the morning, and now the afternoon, I think that medical privacy has been discussed in somewhat abstract terms as though the diminution of privacy in the medical area was something that was unfortunate for the individual; it might cause pain, it might cause embarrassment, could expose somebody to discrimination, but that it was something that was an after-the-fact consequence of the violation of privacy.

The point I want to make is that we believe medical privacy is important, because in the absence of an environment in which people are confident that their medical information will be secure and kept confidential, people will not seek medical treatment in the first instance or people will not be candid with their health care provider. And that is very damaging.

Let me just give two examples, one ripped from today's newspaper. The *Washington Post* reports on a Center for Disease Control study which says that 25 percent of the people who get AIDS tests in this country do not return to receive the results, and CDC speculates that a big part of that is the stigma that is associated with AIDS.

A prior study by the Department of Labor found that a majority of women in the study were reluctant to receive genetic screening for breast cancer. There again, a large part of that problem, and the women said in large part, was because they were reluctant to have a piece of paper exist that said that they had this genetic predisposition. They feared that it would be used against them.

It is not just the after-the-fact consequence. It is that people will not receive the health services that they need. As a result, the work that this committee is doing in this area is as important for individual health and for public health as anything that your colleagues on the Health Subcommittee and the Commerce Committee might be working on at this moment.

That said, I don't want you to be left with the impression that the ACLU thinks that the only issue that needs to be addressed with respect to Gramm-Leach-Bliley is medical privacy. We regretted the fact that your bill, Mr. Chairman, the landmark Gramm-Leach-Bliley bill, did not comprehensively address privacy issues to our satisfaction, and we urge that in this Congress, and as soon as possible, the Congress return to the privacy issues across the board with respect to financial institutions including medical privacy. We think your bill is very good, as my colleagues have stated, but we think applying the principles, especially the opt-in principle, to financial privacy across the board would be even better.

I would just want to quickly highlight three improvements that I don't believe have been mentioned before, and I will say them in very bullet form.

First, with respect to the right to access and correct information, your bill, Mr. Chairman, permits consumers to do that with respect to records that are in the possession of the financial institution. The Ranking Member's bill goes a step further and says records that are under the control of the financial institution and reasonably available, which is a standard that I think is not burdensome and would ensure that financial institutions don't play shell games with the records. If there is to be a right of access and a right to correct, it should apply to all records that are under the control and reasonably available.

Second, there has been discussion about the mental health protections in the bill and we commend you, Mr. Chairman, for putting those in there. I think there was some discussion earlier when Congresswoman Roukema was here about why that would be important. Understand that under the opt-in model, it is very often the case that the opt-in will occur in advance; that when the consumer signs up for the financial product, he or she will be asked to provide consent for the future use of the information. As we read the mental health protection, the special heightened protection in your bill, the financial institution would, if it wanted to use mental health information in the future, would need to come back to the consumer and seek consent for that specific use. We think that is vitally important and we would respectfully suggest that those special protections be extended beyond mental health to other sensitive areas like substance abuse and reproductive health, because those are areas where the fear of embarrassment and discrimination is so great that people are reluctant to seek the health service in the first place.

And, finally, nobody has emphasized the importance of genetic privacy protections. There again, the breast cancer example is one that we are all very familiar with. But the map of the human genome is about to be completed within the next couple of weeks is what we have been told. We think it is vital for Congress to address the circumstances under which that information is going to be available and the circumstances under which it is going to be used.

We strongly support Congresswoman Slaughter's bill to provide those protections, and while not within the jurisdiction of this committee, of course, we think that revisiting the privacy issue, the privacy issues raised in the insurance context under Gramm-Leach-

Bliley, presents an excellent opportunity for the Congress to look at the important issue of genetic privacy. Thank you.

[The prepared statement of Ronald Weich can be found on page 220 in the appendix.]

Chairman LEACH. Thank you very much.

I must say, all your testimony has been extraordinary and very much appreciated. As we move forward, it will certainly be borne in mind, so any very specific language you want to suggest we will look at as well. Feel free to contact us directly.

John.

Mr. LAFALCE. Thank you very much, Mr. Chairman.

A couple of observations. First of all, I thought the presentations of this panel were just outstanding and I thank the Chairman. I requested each of the six of you as witnesses. I think we would have been remiss if we didn't hear from your perspective. I wish more were here to listen to you, both sitting here and sitting out there.

You have been supportive of the Chairman's bill and my bill similarities and differences in approach, but you have also had some suggested changes for both the Chairman's bill and my bill, and we are grateful for that, because whatever we do, we both recognize that we don't have any particular monopoly on wisdom and anything that we have introduced can always be improved.

You have pointed out they can be improved significantly, even in the bill that I introduced on behalf of the Administration. I don't think it goes far enough in certain very, very key respects.

Ms. Breitenstein, you pointed out how very imperative a private right of action is, because if my privacy rights are protected, my personal privacy rights, my property rights, then I don't want to have to rely on the FTC, I don't want to have to rely on the State attorney general, which I have to do even under my bill. I ought to have a right to seek individual redress, because I am the one who has been abused. I don't think that is unreasonable. I think arguments to the contrary are unreasonable. I hear them saying this a defect in my bill even. We need to go further.

Ms. Breitenstein, I point you out in particular, because you made the point that you come from the private sector. There is something else I think that we must get across, and maybe you could help me buttress this point: By promoting privacy, we are promoting good business practice. How many times have you run into individuals who would have used the internet, for example, who would have used some electronic form of commerce, if they didn't have to share personal information; but they get to that point and then they stop. And I think we could have an exponential growth in utilization of the technology that exists if we adopt the strongest possible privacy protections, rather than thinking that the privacy protections will impede that growth. Anyone want to comment on that?

Ms. BREITENSTEIN. I want to thank you for that comment, because it is incredibly astute and, statistically speaking, you are right on the money, so to speak. A 1999 consumer's legal study found that 70 percent of people were unwilling or reluctant to divulge personal information online. A 2000 poll found that 40 percent of women have never made a purchase online, citing privacy as their number one concern.

I wish I had a terrific little vignette for you, but, statistically speaking, if we don't solve privacy, we are not going to support the government of e-commerce and communication and everything else that we want to do online, especially in the health field.

Mr. LAFALCE. I thank you. Let me just—Mr. Hendricks? Before you respond, Mr. Hendricks, let me just say with respect to Mr. Hendricks and I, we didn't just start talking about privacy six months ago. I remember two years ago we were at the White House at a press conference with Vice President Gore, when we were having a press conference about the need for promoting privacy rights at that time. And then I remember the 1970's, working on privacy when Mr. Hendricks was covering it and I was particularly working on that with then-Congressman John Cavanaugh of Nebraska. But you wanted to comment on the buttress, I think, Ms. Breitenstein's point.

Mr. HENDRICKS. The other statistic is something between 70 and 75 percent of the people are filling things up in shopping carts when they go online, and abandon the purchase at the point they are talking about actually having to put their credit card number down. So there is a real perception, fear, hurdle, that has to be overcome and that is why I think we need something dramatic and comprehensive.

You noted that Ms. Breitenstein is from the private sector. There is an exciting dynamic going on. There are new models of companies coming in with the new economy that are based on protecting and enhancing privacy. I am talking to some of those companies, too, and I look forward to sort of bringing them into the debate here to be able to demonstrate how—where in the past you could only make money by invading privacy, and now there is value in protecting privacy.

Mr. LAFALCE. I think I read or heard someplace about a San Francisco company that has a patent that has been issued that would assist in the protection of privacy by scrambling this information. Do you have anything you want to share with us on that?

Mr. HENDRICKS. It is a company I am talking to that has a patent for scrambling credit card numbers, and all through commerce, the merchant, the e-commerce, systems communication, you don't see the real credit card number. It scrambles it so it only goes through and then is confirmed by the acquiring bank and issuing bank. It would be a real technological plus to get this sort of technology into the marketplace. It is going to take a mix of technology and legislative solutions to finally show the American people that we can protect privacy.

Mr. LAFALCE. Let me in closing again thank you, and let me just make a personal observation. This is June. I am not sure whether we will be able to, if we report a bill out, advance it to the floor. I am not sure, given the composition of the Senate and the late legislative schedule, we will be able to advance anything at all in the Senate. Those are just question marks.

The question is: What should we do now and next? A number of you have been very kind in your comments, both toward the Chairman and myself. I don't know what is going to happen in the future. I don't know whether I will be reelected. Assuming I am, I will expect I will be either the Ranking Member or the Chairman

of this committee. Assuming Congressman Leach is reelected, because of the rules of the House, he will not be Chairman in the next Congress. Maybe he could be Ranking Member, I don't know. But if the Republicans have the Majority, it will probably be Ms. Roukema or Mr. Oxley or Mr. Baker, God only knows. But I don't think there is ever going to be a Chairman and Ranking Member who are so similarly disposed substantively on such an extremely important issue, and also of similar personal disposition. And I would hope that we could take this opportunity to craft something that is better than both our bills and as broad and comprehensive as possible, because we might not ever have another opportunity. I thank you and I thank the Chair very much.

Chairman LEACH. Well, thank you, John. Let me thank you all again. Your comments have been splendid. Thank you.

The hearing is adjourned.

[Whereupon, at 2:05 p.m., the hearing was adjourned.]

APPENDIX

June 14, 2000

CURRENCY

Committee on Banking and Financial Services

James A. Leach, Chairman

For Immediate Release:
Wednesday, June 14, 2000

Contact: David Runkel or
Brookly McLaughlin (202) 226-0471

Opening Statement
Of Rep. James A. Leach
Chairman, House Banking and Financial Services Committee
Hearing on H.R. 4585

The Committee meets today to hear testimony on H.R. 4585, the Medical Financial Privacy Protection Act, which would protect the most sensitive information about an individual that is held by a financial firm.

Before summarizing this proposal let me review the legislative background of this issue.

Last year, in consideration of H.R. 10, the Financial Services Modernization Act, this Committee for the first time in the long history of bank reform legislation approved a privacy package. In addition to erecting privacy shields for American financial services customers, including a ban on the transfer of information to third party telemarketers and a clamp down on identity theft, that bill, as it left this Committee contained a provision that would have walled off the medical records held by an insurance company from other affiliates of a financial services holding company, as well as non-affiliated third parties.

H.R. 10 passed the House with the strongest privacy protections ever incorporated into banking law, importantly including the medical privacy provisions that originated in our Committee. Later, however, at the request of the Administration and the insistence of the minority party on the floor that the issue be addressed through executive action rather than legislation, the medical privacy provisions were dropped from the final version of the bill.

Now, it appears that consensus is developing among the interested parties in the government on the desirability of moving forward with a legislative approach to medical privacy. In this regard, the language of H.R. 4585 is consistent with the medical privacy recommendations forwarded to Congress by the Treasury Department six weeks ago and responds to the concerns outlined by the President in his April 30 speech at Eastern Michigan University in Ypsilanti. And in an important disclosure area that deals with information concerning mental health or conditlon, H.R. 4585 goes beyond the Administration recommendations.

The legislation is also consistent with the financial industry accord announced last week. The industry is to be complimented for agreeing voluntarily to provide a credible degree of privacy protection of the medical records of their customers. Some would even contend that because of this voluntary agreement and because of the industry's general record of safeguarding medical records, any legislation represents a solution seeking a problem.

Yet, the background of legislative concern in this area relates less to any history of past industry abuse or of new financial industry organization, but rather to the implications of modern information technology as it relates to new genetics science advances. So much more can now be known about and predicted about individuals based on medical testing that it is important to put common sense restraints in place before temptingly improper industrial practices begin.

The major provisions of the bill, H.R. 4585, which is the principal subject matter of the hearing, are as follows:

- Financial institutions will be required to obtain customer's affirmative consent ("opt in") before disclosing individually identifiable health information to an affiliate or non-affiliated third party.
- A financial institution will be prohibited from obtaining or using individually identifiable health information in deciding whether to issue credit, unless the prospective borrower expressly consents.
- Information relating to mental health or mental condition will be singled out for particular protection with separate and specific customer consent required to disclose such information, and special policies developed by regulators to protect its confidentiality.
- Consumers will be given the right to inspect, copy, and correct individually identifiable health information that is under the control of a financial institution.
- Strict limitations will be placed on the redisclosure and reuse of individually identifiable health information legitimately obtained by a financial institution.
- Nothing will be done to modify, limit or supersede medical privacy standards promulgated by the Secretary of Health and Human Services pursuant to authority granted under the Health Insurance Portability and Accountability Act.

The approach contemplated in H.R. 4585 is designed to augment the privacy provisions of the Financial Modernization bill passed last year. Rules to implement those privacy protections are in the process of being implemented by the Executive Branch, and I believe I can speak for all Members of the Committee in encouraging the regulators to move expeditiously so that all Americans can be more secure in the privacy of their financial information.

Before hearing today from the Administration, government officials, industry representatives and privacy groups on their perspectives on this matter, let me ask Mr. LaFalce if he has an opening statement.

######

Opening Statement
H.R. 4585 – Medical Financial Privacy Protection Act
Rep. Stephanie Tubbs Jones

Good Morning, Chairman Leach, Ranking Member LaFalce and Members of this Committee. Mr. Chairman, I ask unanimous consent that my full statement be included in the Record.

I want to thank Chairman Leach for his outstanding leadership of the Banking Committee, in general, and more specifically his leadership in moving H.R. 4585, Medical Financial Privacy Protection Act, forward to a hearing.

Consumers of this nation deserve better privacy protections with respect to medical and financial information and records. In the midst of Gramm-Leach-Bliley, growth of the internet, speed at which information travels and coupled with the increasing numbers of corporate mergers and subsidiary structures today, consumers desperately need privacy protections.

While there is much still to be learned about consumers' views on the collection and use of personal information in the online environment and between entities, it is possible to discern some general trends. Survey research conducted over the last twenty years documents deep concern among Americans about how personal information is being used.

- 82% stated that they are concerned about threats to their personal privacy
- 78% believe that consumers have lost all control over how businesses circulate and use personal information;
- 66% believe businesses ask consumers for too much information

There are benefits of online technology in the areas of health care and financial services. Electronic transmission of medical information can enhance the quality of health care by facilitating long distance consultations and allow doctors to use email to monitor patients compliance with treatment. In addition, online technology could assist consumers by making financial information that is currently available only through intermediaries instantly available to them.

However, some concerns exist as well. There is a genuine concern about unauthorized access to sensitive medical and financial information. Companies with health affiliates can easily "cherry pick" clients for benefits plans, thus leaving those with a history of health and health related illnesses with no coverage or very expensive coverage. The confidentiality of medical records could be compromised and misued by third parties who gain access through chat rooms, bulletin boards and other means.

Also, there is concern about the commercialization of financial and medical information. Medical information should never be disclosed or used for marketing purposes, unless there is voluntary consent and knowledge.

I support legislation that lays out clear "notice" regulations. Notice is the first principle in advancing information privacy. Notice should include clear language written or typed in conspicuous form.

Consumer choice. Consumers should be able to exercise choice with respect to whether their personal information is used. There may be disagreement as to how choice is to be exercised, but consumers must have choice. I favor "opt out" provisions that allow consumers to agree not to participate in information sharing, etc. I believe the easiest way to do this is to require affirmative consent prior to any collection or commercial use of a consumer's personal information. Individual do have a property interest in their personal information.

I believe H.R. 4585 is a positive step forward to providing consumers with protections regarding to their personal financial and/or medical information. I hope that this hearing today is not taken lightly. There are many constituents in my districts who are deeply concerned about how big business, now with access to their medical records, will use it against them.

I realize today, in our technological society, that security of personal information is essential if commerce in cyberspace is to flourish. Consumers should have access to information about them and determine whether information can be shared with third parties. We, as members of this committee and Congress, have a responsibility to continue to protect consumer interests relative to this sensitive topic. We must enact legislation, like H.R. 4585, that helps to clear up shades of gray relative to information sharing of records and determining the appropriate balance for the consumer relative to their property and privacy rights.

I support the Chairman's legislation and look forward to this hearing.

Statement of Congresswoman Sue Kelly
Hearing on H.R. 4585, the Medical Financial Privacy Protection Act
June 14, 2000; 10:00 a.m.; Room 2128, Rayburn

Thank you Mr. Chairman.

Chairman Leach, Mr. LaFalce I would like to thank you both for agreeing to hold today's hearing on the important issue of medical records privacy. Privacy of our medical records should be an established right -- this is common sense. Medical information constitutes the most personal of information, which should not be shared without the clear consent of the individual.

Around this time last year the House passed H.R. 10, an excellent piece of legislation to bring our financial services into the 21st Century. This legislation contained the greatest expansion of privacy in the history of American finance. I believe this was the right thing to do for America. As has been pointed out, some believe that this legislation did not go far enough, and while we can advance legislation to strengthen these provisions, that is a far easier proposition than repealing laws which have gone too far.

Last year the House passed bill contained protections for personal medical information. Unfortunately, this provision was struck in conference. It is time for that mistake to be corrected.

Chairman Leach has done an excellent job of crafting the bill we have before us today. The Medical Financial Privacy Protection Act will correct the mistake made last year. Of course, as with most legislation we can always polish the edges. I hope that in this process I can work with members on both sides of the aisle to firmly establish a reasonable middle ground. On an issue of such importance it is far too easy to establish positions from which one can claim that the legislation goes too far or not enough. I hope we can all come together in a mutual effort to move this legislation forward.

In some cases it is necessary to provide personal medical information to insurance companies, this practice should not be hampered. Insurance companies must be able to make clear determinations of risk when considering life insurance policies. But beyond these legitimate activities this information must be kept confidential.

I thank the witnesses for taking the time to join us here today to share with us their considerable knowledge so we can arrive at a solid, mutually agreed on piece of legislation. I look forward to discussing these issues with them.

Again I thank the Chairman and yield back the balance of my time.

Statement of

HON. JOHN J. LaFALCE

Hearing on the H.R. 4585–Medical Financial Privacy Protection Act
Committee on Banking and Financial Services

June 14, 2000

Mr. Chairman, this morning's hearing continues this Committee's work on financial privacy which we began two years ago when you introduced legislation which I co-sponsored to prohibit pretext calling and other privacy abuses, and I introduced a related bill to impose obligations on financial institutions to protect the confidentiality of customer information. I am pleased to say that both proposals were enacted into law as part of last year's Financial Modernization legislation in much the same form as they were originally introduced.

This year I introduced H.R. 4380, a comprehensive proposal developed in concert with the Administration to address financial privacy broadly. H.R. 4585, which the Chairman has introduced, addresses only one issue–medical privacy–by restricting the use and disclosure by financial institutions of personally identifiable health and medical information. This is an issue not included in the legislation adopted last year and not adequately addressed in pending HHS privacy regulations.

Both H.R. 4380 and H.R. 4585 reflect the growing bipartisan recognition that the privacy protections adopted last year do not go far enough in assuring that sensitive personal information will be protected by financial institutions and that additional protections must be enacted.

The issue of medical financial privacy eluded us last year. The Committee did adopt a narrow provision to restrict the use of health information in connection with credit decisions that was replaced by a broader bipartisan financial privacy proposal on the House floor. A Commerce Committee proposal to restrict the disclosure of health-related information by insurance companies–the so-called "Ganske" provision–was omitted in conference in response to strong bipartisan concerns that it might preempt pending HHS privacy regulations, preempt stronger state medical privacy laws, and permit widespread sharing of sensitive health data under a broad exception for health research. All the major medical and hospital associations, patient and consumer groups and privacy advocates agreed that the Ganske language created greater potential privacy problems than it resolved.

Both H.R. 4585 and H.R. 4380 are meritorious proposals. In many respects, H.R. 4585 is comparable to the medical privacy provisions of H.R. 4380. I do have some concerns, however, that I'm sure can be worked out, about specific details of this bill.

But, the primary limitation of H.R. 4585 is that it applies only to medical and health information. The higher standard of protection for sharing of consumer profiles

and lists should apply to all sensitive financial and health information. The new protections for consumer access and correction should apply to all sensitive financial information. The stronger standards for reuse and redisclosure of information should apply to all sensitive financial information and not just health or medical information.

In short, H.R. 4585 is a good effort, but we clearly need to do more. If consumers don't want their financial account information shared with affiliated companies without their knowledge, we need to do more than this legislation. If consumers object to having their spending habits and product preferences monitored and sold or shared for marketing purposes, we need to do more than this legislation. If consumers don't want health and insurance information taken into consideration for investment or employment decisions, we need to do more than this legislation. If American consumers want to have the same privacy rights being given to European customers of U.S. institutions, we need to do more than this legislation. And if consumers want the right to determine if their financial records are accurate and up to date, we must do more than this legislation.

I urge today's witnesses not to confine themselves solely to the topic of medical privacy, and would welcome any comments on the broader aspects of the Administration's privacy proposals as contained in my bill, H.R. 4380, or any other proposals that are needed to assure the strongest possible privacy protections for America's consumers.

I thank the Chairman for accommodating the Minority's requests for witnesses for today's hearing–all of whom, unfortunately, are in the fourth panel–and I join with the Chairman in welcoming all of today's witnesses.

Opening Statement of
Honorable Barbara Lee
Full Committee on Banking and Financial Services
Hearing on H.R. 4585, the Medical Financial Privacy Protection Act
June 14, 2000

Thank you, Mr. Chairman and Mr.LaFalce, and thank you to our guests who have come here to speak on the right of individuals to medical privacy. Consumers have real and legitimate concerns about medical privacy and financial institutions.

In the relationship between our financial institutions and the consumer the core value of must be trust. Financial institutions cannot succeed without the trust of their customers.

I commend the Chairman for his proposal and I recognize the importance of this issue. However I feel that we as a body should be doing even more to insure the privacy of our citizens. I especially feel this is important when dealing with the privacy of medical records.

Medical records are a sensitive subject. Our constituents count on us to ensure that this system remains private. Information about physical and mental health should not be exposed to the prying eyes of credit checks or other financial transactions. We should be able to tell our constituents, "your records are safe."

As we discuss medical privacy, we should consider the present administration's privacy initiative, which offers a more comprehensive approach to medical privacy for consumers.

Thank you, Mr. Chairman and Ranking Member LaFalce, for having this hearing on this important matter, and thank you to our guests for coming here and speaking to us today.

House Banking Committee
Opening Statement
Rep. Carolyn B. Maloney
June 14, 2000

Thank you Mr. Chairman for holding this critical hearing on consumer privacy. I truly hope this is a sign that the House Republican leadership is prepared to provide consumers with greater privacy protections this Congress.

The importance of this issue is underscored by the E-sign legislation on the floor of the House today. This legislation will allow increased commerce to be conducted over the Internet.

It also underlies the important balance that must be struck in legislating new privacy protections. Consumer's financial and medical information must be accorded significant legal protections but privacy must be crafted so that the pace of electronic commerce is not slowed.

Without additional privacy protections, electronic commerce, and especially Internet-based financial services, could be undermined if consumers are not confident that their privacy is being protected.

Last year this Committee took a small first step in ensuring that consumer privacy is protected as financial institutions continue to merge and as the economy becomes increasingly digital.

These were simple common sense protections that give consumers the opportunity to review their financial institution's privacy policies and the opportunity to restrict the sharing of their information from third-party marketers.

The Chairman's bill includes some key principles - especially that credit decisions should not be based on health information. However, I would hope that as this Committee continues to work on consumer privacy that Rep. LaFalce's legislation providing comprehensive financial privacy protections is a focus of our consideration.

Thank you Mr. Chairman. I yield back the balance of my time.

Statement for the Record
House Committee on Banking and Financial Services
Hearing on the Medical Financial Privacy Protection Act, H.R. 4585
Rep. Edward J. Markey (D-MA)
June 14, 2000

Chairman Leach, and Ranking Member LaFalce, I thank you for the opportunity to testify before you today on one of the most important issues facing our nation.

Privacy. The right to be let alone. One of the most basic values of our society – an old value threatened by a new economy. The question of the hour is how to best approach protecting this value we hold so sacred? How to animate our new economy with our old values. How to create commerce with a conscience.

In the past, privacy concerns triggered thoughts of George Orwell's *1984*, where the greatest threat to privacy was Big Brother – the government. Today, the principal threat to personal privacy comes from the desire to earn Big Bucks. Corporate greed is what drives today's threat of our "right to be let alone". And because of this, we have fewer and fewer privacy keepers and more and more personal information reapers.

Right now, when it comes to your financial records, there are very few protections to prevent a financial services firm from disclosing every check you've ever written, every credit card charge you've ever made, the medical exam you got before you received health insurance. And as you surf the Web, there are no rules in place to prevent various web sites from collecting information about what sites you are viewing and how long you are viewing them. If you buy anything over the Internet, that information can be linked up to other personal identifiers to create a disturbingly detailed digital dossier that can profile your lifestyle, your interests, your hobbies, or your habits. The name of the game is Profiling for Profits and in this game we all lose –we lose our right to keep our personal information private.

With the passage of last year's financial services bill (Gramm-Leach-Bliley Act) the barriers between banks, insurers and securities firms have crumbled allowing for the free flow of information between these newly created affiliates. The Gramm-Leach-Bliley Act provided very weak privacy protections to consumers, giving them no right to "opt out" of having their personal, nonpublic financial information transferred to "affiliated" third parties. Furthermore, there's a "joint marketing agreement" provision that allows disclosures of a customer's information to nonaffiliated third parties with which the institution has signed a contract. These two loopholes severely compromise the limited "opt out" requirements in the bill. And just a few weeks ago, we learned that the financial regulators have decided to delay full implementation of even these minimal privacy protections until July 2001.

So you see, the potential for invasions of privacy are everywhere, when you click on a web site, when you pay with a credit card, when you visit your doctor and share your medical information.

Health information is perhaps the most sensitive information about you and your family. When I ask you to picture your medical record I would bet that many of you picture something that looks like a file folder containing the documentation of your health history which likely could include some of the most personal and intimate details of your life. You probably imagine this record in your doctor's office or your local

hospital locked away in a filing cabinet, the keys to which dangle around the neck of a trustworthy nurse who looks like your mother, the guardian of your medical information. But as I've explained here today, there is little in federal law to protect your personal information and this includes your medical information.

Health information privacy has been of great concern to me. Last year I introduced a comprehensive medical privacy bill – the Medical Information Privacy and Security Act, H.R. 1057. The Senate companion bill S. 573, was introduced by Senators Leahy and Kennedy. In addition, I joined Mr. Condit, Mr. Waxman and Mr. Dingell in introducing the Health Information Privacy Act, H.R. 1941.

When these bills were introduced, we were hopeful that Congress would meet the Health Insurance Portability and Accountability Act (HIPAA) deadline to pass meaningful medical privacy legislation by August 1999. Unfortunately, Congress failed to act. Consequently, HIPAA required the Secretary of Health and Human services to promulgate health privacy rules – however the statute limits HHS's coverage and scope. Only electronically transmitted information is covered, and only health information within a health care provider, a health insurer and health data clearinghouses.

Given the threats to health privacy that the Gramm-Leach-Bliley Act left unaddressed, I commend the Chairman's efforts to protect sensitive health information through the bill H.R. 4535. However, just as we need a broad approach to medical privacy, I believe we also need a broad approach to financial privacy. Unfortunately, Mr. Leach's privacy bill fails to protect all information housed in a financial holding company and it fails to close the gaping loopholes under the financial services bill which allow for the sharing of personal financial information with affiliates and non-affiliated third parties. Under the Leach bill, a customer has no right "opt-out" of the sharing of personal financial information that provided to a bank when filling out a loan application or to a securities firm when opening a brokerage account.

Last November, I introduced The Consumer's Right to Financial Privacy Act, H.R. 3320 to close the privacy loopholes created by Gramm-Leach-Bliley and to provide strong, comprehensive privacy protections for all personal information. Currently the bill has the bipartisan support of 71 Members. I am also a lead cosponsor of The Consumer Financial Privacy Bill, H.R. 4380, introduced by Ranking Member LaFalce. This bill also provides comprehensive protections for all personal information and requires an "opt-in" for medical information and personal spending habits. It also closes the Gramm-Leach-Bliley privacy loopholes which allow for privacy assaults on personal financial information.

Participation in the new economy shouldn't come with the price of privacy. In creating commerce with a conscience, we need to do more – not less-- in protecting our personal information. I urge this committee to support a more comprehensive approach to protecting all personal information within a bank holding company, and to support closing the gaping privacy loopholes which exist in our current law.

I thank you for this opportunity to express my views and look forward to working with you on this extremely important issue.

# # #

OPENING STATEMENT
Hon. Marge Roukema

Hearing on the "Medical Financial Privacy Protection Act"
June 14, 2000

Today the Committee will be addressing a topic that is important to all Americans—the right to expect that personal health and medical records will remain private. I thank the Chairman for holding these important hearings.

At the outset, I want to remind everyone that I strongly supported the landmark financial privacy protections in the Gramm-Leach-Bliley Act. They are important protections and serve as a strong foundation on which we most likely will have to continue to build. In crafting these protections, I worked closely with my colleagues on both sides of the aisle: Mr. LaFalce, Mr. Vento, Mr. Oxley, Ms. Pryce, and Mr. Frost. In the end, the House approved the privacy protections by an overwhelming 427-1 margin. Clearly, Congress has shown that it recognizes the importance of privacy protections and can work together in a bipartisan basis. The regulatory agencies have recently issued final rules implementing these financial privacy provisions. My Subcommittee will be holding oversight hearings on these rules in late-July. It is my opinion that additional legislation relating to the privacy of financial records is not appropriate until the regulators gain some experience operating under the final rules.

Today, however, we specifically address the privacy of medical records. I want to emphasize that fundamental medical privacy protections were originally included in the House-approved version of the financial modernization bill. To further analyze this issue, my Subcommittee held two days of hearings last July on both financial and medical privacy. We heard then from many of the same witnesses that we will hear from today. At that hearing, some of the witnesses expressed concerns relating to the medical privacy provisions. I supported working out the areas of concern discussed at the hearing during the House/Senate Conference so that the medical privacy provisions were kept in the bill. However, at the insistence of the Administration and my Democratic colleagues, the medical privacy protections were dropped from the bill during the Conference. Now it is our job to determine how best to move forward on medical privacy protections in separate legislation. It is critical that political considerations not undermine our efforts, and I believe that we will be able to work together in a bipartisan manner.

I should emphasize at this point that addressing medical privacy protections is a complicated issue. There are several substantive concerns that must be addressed that I hope the witnesses will discuss with specificity. Questions that need to be answered include: Are the limits on re-use of medical information adequate? Are the exceptions to the prior notification and consent requirement tailored to ensure that there are no loopholes? What is the status and the scope of medical privacy standards being developed by HHS under the authority of the Health Insurance Portability and Accountability Act? How can industry concerns over the consumer's right to access and correct medical information held by a financial institution be resolved? I look forward to today's testimony for guidance on these issues, and with that, I yield back.

TREASURY UNDER SECRETARY GARY GENSLER
HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

Mr. Chairman, Ranking Member LaFalce, and Members of the Committee, thank you for inviting me here this morning to present the Administration's views on personal financial privacy. I am pleased to have the opportunity to discuss these important issues, and to comment on H.R. 4585, the Medical Financial Privacy Protection Act introduced by Chairman Leach last week.

Protecting consumers' privacy is of the utmost importance to the President and the entire Administration. We want to work with Congress to provide Americans with the comprehensive financial privacy protections they expect and deserve. Our financial system's future growth rests in no small part on continued consumer confidence. Effective privacy protections are an important foundation for that confidence. While we made some significant progress toward this goal in the financial modernization bill signed by the President last year, we believe more work can and should be done in this area.

To that end, the President announced an important new legislative proposal in April, 2000 to provide Americans with fully effective financial privacy protections. The plan enhances consumer choice and control in several important ways. In particular, it provides special protections for especially sensitive information, including the use of medical information in financial settings.

My testimony is divided into four main parts:

- First, I will discuss the importance of privacy protections and the changes in the financial services industry that are making this an ever-more important issue.

- Second, I will review last year's efforts to improve personal privacy protections, including the provisions in the financial modernization bill.

- Third, I will outline the President's comprehensive Consumer Financial Privacy Act initiative.

- Finally, I would like to comment on medical privacy, and discuss the bill introduced last week by Chairman Leach.

I. The Importance of Privacy in America's Changing Financial Markets

Personal privacy is a fundamental and highly prized American right. From our nation's earliest days, citizens have been concerned about intrusions into their private lives, and have fought to protect themselves from unwarranted invasions of their privacy. Over time, ideas regarding what constitutes appropriate privacy protection have changed as our society and economy have evolved.

Many Americans increasingly feel their privacy threatened by those with whom they do business. These concerns are particularly acute when it comes to the privacy of financial information, because financial data can be used to paint such a detailed portrait of an individual's life. Financial institutions and other firms are able to consolidate and process information about individuals' spending and investing habits in ways that were almost inconceivable even a decade ago.

These capabilities are increasing public anxiety about just who has access to sensitive financial information, and what they will be able to do with it. A significant majority of Americans are deeply concerned about the effects that changes in technology are having on their ability to preserve, in the words of Justice Louis Brandeis, "the right to be let alone."

Americans want the ability to earn, invest, and spend their money without having to worry about that information being obtained - and perhaps used to their disadvantage - by firms unknown to them, or having that information open to inspection by the world at large. Just as we do not expect letter carriers to read our mail, we do not expect financial institutions to amass information about our transactions, consolidate and process it, and use it for purposes that we never intended. We are in the midst of three sea-changes in the financial services sector, however, that make such uses of information an increasing possibility: industry consolidation, a technological revolution, and a move away from cash towards electronic transactions.

Changes in Industry Structure. Integration and consolidation in the financial sector is changing the outlook for data privacy. Banks have moved into insurance and securities activities, insurance companies offer products that compete with bank products, and investment banks are in the lending business. Thanks to the hard work of Chairman Leach, Ranking Member LaFalce, Members of this Committee, and many others, last year the President was able to sign into law a financial modernization package that finally eliminated legal barriers to this consolidation. These changes will bring considerable benefits to consumers in the form of increased competition and greater innovation. The desire of integrated financial services firms to profit from their scale has created a powerful incentive to treat consumer data as a business asset, however, which raises concerns about how that information will be used and controlled.

Technological Advances. Changes in technology have brought the ability to generate, process, and use information in ways unimagined when most of our commercial and consumer protection laws were written. These advances have been particularly important in the financial sector, where firms are spending billions of dollars each year on computers and software to reduce costs and improve service. These increasingly sophisticated tools and larger stores of transaction and other financial information, however, have given consumers pause about the potential uses of the data held by banks, insurers, and other financial firms.

The Move to Electronic Transactions. Finally, the explosion in the use of electronic payments and receipts is also driving concerns about data handling and use. Americans' increasing use of credit cards, debit cards and (more recently) electronic bill payment in lieu of cash now allows financial services companies to collect a far greater amount of information on each individual's transactions.

Taken together, these three trends – industry consolidation, technological advances, and the movement from cash to electronic payments and receipt systems – provide financial services firms with powerful incentives to mine consumer information for profit, and the tools with which to do so. The challenge, therefore, is to protect the privacy of consumers while preserving the benefits of competition and innovation.

II. Efforts to Enhance Financial Privacy Protections

This Administration took steps to address these challenges in May of 1999, when the President announced his plan for Financial Privacy and Consumer Protection in the 21st Century. That initiative recognized that while many firms collect information about us, financial institutions have access to a unique window on the lives of most Americans. While a grocery store may learn something about the food you buy, and a department store may know what kind of clothes you prefer, banks, insurers, and brokerage firms collect a range of information that is particularly comprehensive and personal. By processing all of your transactions, a bank or credit card company can know much more about you than any individual merchant. This information can also be particularly sensitive. A list of each prescription drug you purchase or each stock you buy is more revealing – and potentially more open to misuse – than a list of the music CDs you buy.

With this in mind, the President recommended legislation to provide consumers with notice and choice before their financial information is shared or sold -- the right to say "no" to uses of information that individuals find invasive or inappropriate. Central to this policy is the idea that a consumer's financial information belongs to the consumer, not the financial institution that processes the transactions.

At the time this announcement was made, in the midst of the financial modernization debate, the President's agenda struck many as ambitious. Some suggested that the American people did not feel particularly strongly about privacy issues, and that in any case Congress was not prepared to act on legislation in this area. Clearly, the last twelve months have shown otherwise.

Although privacy was not initially part of the financial services debate, this Administration felt strongly that if the rules for industry structure were being modernized, critical protections for consumer data had to be updated as well. The final bill made progress toward that goal. We believe that the new law's requirements for clearly stated privacy policies, for effective notices to consumers, and for the right to opt-out of third-party information sharing are important advances in privacy protection for all Americans.

This Administration believes, however, that much more can and should be done on financial privacy. When the President signed the financial modernization act, he said, "I do not believe that [its] privacy protections go far enough." He continued, "Without restraining the economic potential of new business arrangements, I want to make sure that every family has meaningful choices about how their personal information will be shared within corporate conglomerates. We can't allow new opportunities to erode old and fundamental rights."

III. The Consumer Financial Privacy Act

On April 30, 2000, the President announced a new initiative to provide Americans with the additional protections he promised. That legislation is now before Congress as H.R. 4380, the Consumer Financial Privacy Act. This bill takes a balanced, comprehensive approach to financial privacy, providing important new rights and protections while addressing deficiencies in last year's legislation. I would like to take a few minutes to describe the proposal.

Opt-In Protection for Especially Sensitive Information. A central Administration principle regarding privacy is that the greater the sensitivity of the data and the possible harm from misuse, the greater should be the level of privacy protection. The Consumer Financial Privacy Act therefore calls for the strongest protections in two highly sensitive areas: the sharing of medical information by financial institutions, and the use of detailed personal spending habits information about individual consumers. In these areas we have set the bar high, requiring institutions to get affirmative ("opt-in") consent from consumers before information sharing can occur.

- **Medical Information.** A consumer seeking a loan or other financial products such as investment advice or auto insurance should not have to worry that an institution is making decisions based on personal medical records received from a life insurance affiliate. Life insurance databases should not become the new source for marketing campaigns based on medical information. The Consumer Financial Privacy Act would assure that companies do not gain any special access to medical records by being part of a financial holding company. Consumers would have to give affirmative consent before any financial firm could even receive medical information from a life insurance affiliate or other company.

- **Personal Spending Information.** Americans do not expect a bank processing checks or credit card payments to take their most sensitive financial information and share that information with others. Under the Administration's proposal, a financial firm would not be

permitted to transfer individualized, personal spending habits – where people spend their money, where they earn their money, and what they buy – unless a customer affirmatively consents to such a use of their information.

Opt-Out Protection for Other Financial Information. For other less sensitive categories of financial information, we believe that consumers should have meaningful choice – the opportunity to opt-out -- before a financial services firm can share their financial data with any other entity for marketing purposes. Last year's legislation granted important rights to opt out of information sales to telemarketers and other unaffiliated firms. The Consumer Financial Privacy Act would extend those protections to information shared within financial conglomerates. In a world where affiliates can engage in activities ranging from data processing to travel agency, consumers deserve to have as much control over flows of information to affiliates as they do over those to third parties.

The Administration proposal would also close the exception for "joint marketing" in last year's bill. This provision would constitute an unnecessary loophole when there is opt-out choice for affiliate sharing.

Exceptions for Important Business Practices. The Consumer Financial Privacy Act would preserve financial firms' ability to share information for important business practices by providing exceptions from consumer choice for transaction processing, risk management, fraud prevention, and to aid in law enforcement. In addition, the proposal will provide a new exception to facilitate the development of innovative customer service tools such as consolidated monthly statements and call-in centers that can access information from affiliated firms at a customer's request.

These exceptions are crucial for the growth of our financial industries. They must be subject, however, to appropriate reuse limitations. We include such limitations in order to prevent abuses.

The Administration's proposal thus achieves the goal of matching the level of protection to the sensitivity of the personal information involved and the potential abuses of such information. For the most sensitive data on health and comprehensive personal spending habits, we call for opt-in consent. For other types of financial information, consumers should have the right to opt-out of sharing for marketing and other purposes. Where important business practices require information sharing, we provide exceptions to consumer choice, but make sure that consumers are protected by reuse restrictions.

Additional New Privacy Protections. Beyond notice and consumer choice requirements, the Administration proposal provides additional protections in several key areas, including:

- The right for consumers to access and correct information held by financial institutions, to ensure that firms are not deciding whether to offer them services based on mistaken information about their financial status;

- Additional enforcement authority for the Federal Trade Commission and State Attorneys General;

- Stricter limits on redisclosure and reuse of customer information; and

- Giving consumers the tools to comparison shop by requiring institutions to provide privacy policy notices up front or upon request.

The Administration strongly favors a comprehensive approach to providing additional privacy protections. We found that last year's bill, as important as it was, did not go far enough, compelling us to call for additional legislation. We feel that our proposal covers the necessary ground, filling the gaps in the financial modernization act, and including important new protections. The American people want and deserve these privacy protections now, for the full range of issues addressed in the President's proposal.

We are pleased that so many members of the House and Senate have supported this approach, and have sponsored these proposals in Congress. Improving financial privacy protections is a priority for so many members of this Committee. I would especially like to thank Ranking Member LaFalce for being the lead sponsor of H.R. 4380 in the House. I also thank the other Members of this Committee who are among the many co-sponsors of this comprehensive legislation.

IV. Medical Privacy and Financial Services

Let me turn now more specifically to the issue of medical privacy in the financial context. This Administration firmly believes that all Americans should be protected against the misuse of their highly sensitive health and medical data. We feel that there is broad agreement in the private sector and among the public that improving medical privacy is the right thing to do.

We are deeply committed to providing consumer control and rigorous statutory safeguards in the area of medical privacy. Congress and the Administration worked together in 1996 to enact the Health Insurance Portability and Accountability Act (HIPAA). HIPAA called for enactment of comprehensive privacy legislation by August 1999, and instructed the Department of Health and Human Services to issue rules if that deadline were not met. President Clinton announced the proposed rules last October. He has pledged that final medical privacy regulations will be issued this year. By its terms, HIPAA applies only to "covered entities" such as health providers, health plans (including health insurance companies), and health clearinghouses. Its protections do not apply to most financial institutions, including life, auto, workers' compensation, property and casualty, and many disability insurance companies. The Consumer Financial Privacy Act and H.R. 4585 would provide the first specific federal protections for medical information in financial institutions that are not covered by HIPAA.

As we have seen in past attempts to address medical privacy in the financial context, it can be difficult to reach solutions that do not have unintended consequences. In last year's financial modernization debate, proposals were offered that addressed some issues, but could have seriously undermined other crucial medical privacy initiatives.

For instance, measures under consideration last year would have preempted the HIPAA regulations that HHS is now in the process of making final. The provisions would have exempted the health information they did cover from the re-use restrictions of the modernization bill, providing a significant loophole for the inappropriate release of confidential health information. They also would have permitted, under the guise of "research," exceptions for the sharing of large volumes of extremely sensitive medical information that would be prohibited under the proposed HHS rules. Ultimately, these provisions were not included in the final bill so that the issues could be examined more thoroughly.

We have looked closely at these issues in the ensuing months, in consultation with HHS and others. We believe that our new proposal provides appropriately strong protections for the use of health information in the context of financial products and services. We believe it meets the central challenges I just mentioned. The proposal:

- Addresses the use of medical information in a broad context, covering the provision of all financial products and services;

- Avoids broad exceptions that could render the protections ineffective; and

- Clarifies that nothing in the financial modernization laws would modify or supersede HIPAA's privacy protections, preserving the effectiveness of these important rules.

H.R. 4585, The Medical Financial Privacy Protection Act

Mr. Chairman, by convening this hearing you are creating a much appreciated opportunity to discuss the important issues surrounding financial privacy. Your legislation is focused specifically on medical privacy. While we continue to believe that it is necessary to seek legislation that provides comprehensive privacy protections, your bill offers a starting point for consideration of several issues that we know will be an important part of a truly effective privacy regime. Your bill, H.R. 4585, seeks to address the privacy of medical information in four primary ways:

- In the context of making decisions about a loan or other extension of credit, an institution may not receive or use health information about a consumer from another company unless it has provided notice and obtained affirmative consent.

- The bill bars financial institutions from disclosing medical information to affiliates or third parties without providing notice and obtaining opt-in consent.

- An institution must obtain affirmative opt-in consent before it can transfer detailed personal health spending information about a consumer to an affiliate or third party.

- Institutions must provide consumers with access to, and the opportunity to correct, individually identifiable health information. The bill also provides additional protections for the reuse of health information, and for mental health information.

Mr. Chairman, we appreciate your personal involvement in this area. You have introduced legislation that furthers the debate on these critically important issues. There is common ground between your bill and the Administration's proposal regarding financial medical privacy. H.R. 4585 does differ in significant respects, however, from the Administration's proposal. While there are a number of other issues, let me highlight our two most important concerns.

Scope of the Bill. We believe that financial privacy legislation should address the full range of important consumer protections. The Administration's Consumer Financial Privacy Act addresses the full range of important financial privacy issues that now face the American people. It would, among other measures, provide opt-in protection for consumer personal spending habits; require customer choice before information is shared among corporate affiliates; provide customers with access to and the ability to correct their financial records; assure that privacy policies will be available for comparison shopping; and enhance enforcement authorities where needed.

H.R. 4585, by contrast, is a narrower bill that addresses only the medical privacy issues covered by the Consumer Financial Privacy Act. Some of the issues I just noted, such as personal spending habits, access, and reuse, are included in H.R. 4585, but solely as it relates to personal health information. Medical privacy within the financial services industry is vitally important, but is only one of the financial privacy issues that must be addressed. American consumers want and deserve a broad set of protections.

Receipt and Use Provisions. The provisions in H.R. 4585 concerning "use or receipt" of medical information apply only to "a loan or credit to a consumer." We feel that it is crucial to apply the privacy protections beyond the "loan or credit" setting. A provision that applies to disclosure and use of health information only with respect to "loans or credit" would permit uses of health information in situations involving marketing and other financial settings. It is unclear why the use of sensitive medical information should be subject to restrictions in the provision of a loan, but not in the provision of investment advice, auto insurance, travel services, or any of the many other non-credit products now permitted in financial holding companies.

An additional provision in the President's receipt and use proposals provides that a financial services firm can only receive or use medical information from an affiliate or third party that it requires of *all* of its customers for a particular product or service. The language in H.R. 4585 that seems to address this same topic is unclear, and may have unintended consequences.

Conclusion

Mr. Chairman, thank you for providing this forum for the discussion of these critically important issues. This hearing provides a starting point for a thorough consideration of the range of privacy issues raised by changes in technology and in our financial markets.

This is a historic opportunity to get financial privacy right - to put in place all of the protections that American citizens want and need. In addition, we all recognize the special sensitivity of personal medical information. The Administration supports having effective laws in place that match the sensitivity of such data. There is common ground between Chairman Leach's bill and the Administration approach. At the same time, we should also address the other vital issues that are included in the Consumer Financial Privacy Act. To do otherwise is to miss out on the chance to complete the work that was begun in last year's law.

We look forward to working with you, Congressman LaFalce, and other Members of Congress to provide all Americans with comprehensive financial privacy protections.

--30--

Testimony
of the
National Association of Insurance Commissioners
Before the
United States House of Representatives
Committee on Banking and Financial Services
on
H.R. 4585
Privacy of Health Information

June 14, 2000

National Association of Insurance Commissioners
David Wetmore, Director
Federal and International Relations
444 North Capitol St., NW Suite 701
Washington, DC 20001-1512
Tel: 202-624-7790
Fax: 202-624-8579

I. Introduction

Good morning, Mr. Chairman and members of the Committee. My name is Kathleen Sebelius. I am the elected Insurance Commissioner for the State of Kansas, and I am testifying today as Vice President of the National Association of Insurance Commissioners (NAIC). I also chair the NAIC's Health Insurance and Managed Care Committee and the NAIC Privacy Issues Working Group, both of which have devoted much time and energy to the subject before us today.[1] I am accompanied by the Vice-Chair of the working group, Glenn Pomeroy, Insurance Commissioner of the state of North Dakota and a past president of the NAIC.

Let me begin by thanking you, Mr. Chairman, for giving the NAIC this chance to testify on the subject of health information and offer our views and comments on your new legislation, H.R. 4585, the "Medical Financial Privacy Protection Act." We have testified five times previously on health information privacy before the 106th Congress.

The NAIC has a long history of working to protect the health information of consumers, and we are now working very actively to guide state implementation of the new Title V consumer privacy provisions under the construct of the Gramm-Leach-Bliley Act (GLBA).

My testimony today will focus on: (1) the need for privacy protection of health information in GLBA; (2) NAIC's activity on privacy and implementing GLBA regulations; and (3) comparison of H.R. 4585 to the NAIC Health Information Privacy Model Act.

---

[1] The NAIC, founded in 1871, is the organization of the chief insurance regulators from the 50 states, the District of Columbia, and four of the U.S. territories. The NAIC's objective is to serve the public by assisting state insurance regulators in fulfilling their regulatory responsibilities. Protection of consumers is the fundamental purpose of insurance regulation.

II. The Need for Privacy Protection of Health Information in GLBA

When you ask consumers about protection of their personal information, they think health information is the most sensitive and expect a greater level of protection for their personal health information. Unfortunately, GLBA does not reflect consumers' legitimate concerns in this area.

Congressman Leach, we are pleased with your decision to recognize that an unintended consequence of GLBA is the fact that a consumer's sensitive health information can be shared freely without distinction from other sorts of financial information. Although we do not believe the intent of Congress last year was to include health information in the final version of GLBA, the implementing regulations have changed the landscape because "financial information" is defined to include health information.

As we all know, limited privacy protections of financial information are included in GLBA's Title V. But with all due respect, these protections fail in the health area because the law does not provide more stringent protection for health information.

While this "opt-out" standard may be adequate in providing privacy protections for banking and financial information (in the true sense of the word), this standard is not adequate for personal health information.

So what kinds of information could be at risk?

While we were developing the health privacy model, we heard horrible stories of how sensitive personal health information was disseminated without the individual's knowledge or consent. For example, a man made a claim against his insurance company for reimbursement of the costs of a drug prescribed for a certain medical condition. Within days, his doctor was besieged by calls from pharmaceutical companies trying to convince the doctor to change the patient's medication to a drug produced by that

particular company. This type of disclosure would be prohibited under your bill and our model without the affirmative consent of the consumer.

For these reasons, we think Congress needs to revisit the GLBA provisions and provide comprehensive privacy standards across-the-board regarding financial institutions and individually identifiable health information.

We think H.R. 4585 is a good step in the right direction to accomplish this goal. Specifically, we agree with your approach, Mr. Chairman, in several key areas:

- health information should be treated separately from, and differently than, financial information;
- individually identifiable health information should be afforded more protection than financial information;
- an "opt-in" standard should be implemented for individually identifiable health information due to the sensitive nature of the information; and
- the standard should be the same for all individually identifiable health information and should not be based on the type of financial institution that holds the information.

These aspects of your bill mirror standing NAIC policy, and we applaud your efforts in amending GLBA to include these important protections that are conspicuously missing now. We believe the best approach on the issue of health information privacy would be to set a federal standard that does not preempt stronger state laws that have been protecting health information for so many years. This approach is consistent with the GLBA standard – state laws are preempted only if they are "inconsistent with" GLBA and stronger state laws are not inconsistent.

III. NAIC Activity

A. NAIC Model Legislation

Members of the NAIC have been discussing and addressing the privacy of personal information, including health information, for more than 20 years. In 1980 we adopted

the Insurance Information and Privacy Protection Model Act (Attachment A). This model applies to all insurance information and generally requires insurers to receive authorization from individuals ("opt-in") to disclose personal information. Health information is specifically included as part of this model.

More recently, in September 1998, the NAIC continued its efforts to strengthen protections for personal information by adopting a new model solely focused on the issues specific to health information, the Health Information Privacy Model Act (Attachment B). This model was developed following an extensive dialogue, over four years, with all stakeholders, including representatives of the insurance and managed care industries, and representatives from the provider and consumer communities.

Our model applies to all insurance carriers and was developed to assist the states in drafting uniform standards for ensuring the privacy of health information.[2] Similar to our more general 1980 insurance privacy model, this health information privacy model generally requires an entity to obtain an authorization ("opt-in") from the individual to collect, use or disclose protected health information. However, this new model treats personal health information as a different type of information that should receive a higher level of privacy protection. It balances the business needs of insurers against the legitimate privacy concerns of consumers.

---

[2] With respect to insurers, we recommend the approach of H.R. 4585 and of the NAIC model, which applies to all insurance carriers and is not limited to health and life insurers. The NAIC had an extensive public discussion about whether the NAIC model should apply only to health insurance carriers, or instead, to all carriers. Health and life insurance carriers are not the only types of carriers that use health information to transact their business. Health information is often essential to property and casualty insurers in settling workers' compensation claims and automobile claims involving personal injury, for example. Reinsurers also use protected health information to write reinsurance. The NAIC concluded that it was illogical to apply one set of rules to health insurance carriers but different rules, or no rules, to other carriers that were using the same type of information. Consumers deserve the same protection with respect to their health information, regardless of the entity using it. Nor is it equitable to subject life and health insurance carriers to more stringent rules than those applied to other insurers. Our model applies to all insurance carriers and establishes uniform rules to the greatest extent possible. The NAIC model requires carriers to establish procedures for the treatment of all health information, and then establishes additional rules for protected health information (individually identifiable health information in H.R. 4585).

We note that your bill would codify these important principles of our new model. We also note that our model could serve as a basis for developing regulations under your bill. Although our model is particular to the insurance business, it is important to remember that insurers are the primary financial institutions in possession of individually identifiable health information. Any regulations drafted under your bill should keep this fact in mind.

B. NAIC's Draft GLBA Regulations

As members of this Committee know, the GLBA directs Federal and State regulators to establish comprehensive standards for ensuring the security and confidentiality of consumers' personal information maintained by financial institutions, and to protect against unauthorized access to or use of such information. Moreover, Section 507 authorizes – some would say encourages – States to enact laws that give consumers greater privacy protections than the provisions of GLBA.

As functional regulators of the business of insurance, the states are working through the NAIC to promulgate a model privacy regulation for the business of insurance. We are doing so in a manner that is as consistent as possible with the federal regulations while capturing the unique business and consumer aspects of insurance. As one of the NAIC's nine commissioner-level working groups, the Privacy Issues Working Group, which I chair along with my vice-chair Commissioner Pomeroy, has been meeting since February to develop a draft regulation although our work began in earnest once the federal regulations were finalized.

We met this past weekend during our Summer National Meeting to discuss a working draft of proposed NAIC interim consumer privacy regulations which are intended to serve as guide for states to satisfy Title V of GLBA. The purpose of these interim regulations is to help state insurance authorities comply with the minimum requirements of GLBA quickly and therefore give to the industry the guidance it needs in this area, while ensuring essential consumer protections.

The draft is based upon the final Federal privacy regulations with regard to consumer financial information. Because of the differences between insurance activities and banking activities, we have made several changes that strengthen the privacy protections for individuals as they relate to insurance, notably with respect to health issues.

Insurance providers typically collect much greater amounts of health information than banks. We have also decided to treat health information differently than financial information and have drafted enhanced protections. This is in accordance with our previously adopted policy standards (as evidenced by existing model laws). As a result, our draft regulations make clear that "financial information" does not include "health information". Having made that distinction, we apply different rules for financial information and for health information. For financial information, we have closely tracked the language in GLBA in drafting regulations for insurers and their treatment of financial information.

For health information, we create an "opt-in" standard to be added to the Federal rules to address the special privacy issues with health information. We then address specific exceptions to the general rule to allow insurers to carry on their day-to-day business operations without undue restrictions. Our intent is to specifically treat personal health information as a different type of information that receives a higher level of privacy protection, as required by the our model.

At our recent Summer National Meeting, the working group discussed the "opt-in" standard for health information. Most insurance industry representatives voiced support for this standard.

We have an accelerated timetable for finalizing this regulation, and we anticipate a final work product by September 2000 so states may implement it by regulation or introduce it as legislation, if necessary, in the next legislative session.

IV. Comparison of H.R. 4585 and the NAIC Health Information Privacy Model

H.R. 4585, which builds upon the privacy protections for financial information in GLBA by adding protections for individually identifiably health information, is similar in several aspects to the NAIC Health Information Privacy Model. Similarities include:

- Treating health information privacy separately from, and differently than, financial information.
- Affording individually identifiable health information more protection than financial information.
- Prohibiting disclosure of individually identifiable health information without affirmative consent ("opt-in") from the individual.
- Giving individuals the right to access and amend individually identifiable health information that is collected by a financial institution.
- Placing strict limitations on the re-disclosure and re-use of individually identifiable health information legitimately obtained by a financial institution.
- Establishing a list of exceptions for certain activities that do not need authorization from the individual. Although the exceptions in H.R. 4585 and the NAIC Model do not exactly correlate (GLBA exceptions geared toward banking business and NAIC Model exceptions geared toward insurance business), each set of exceptions recognizes the needs of financial institutions to use and disclose individually identifiably health information for legitimate business purposes.

While the NAIC model is more detailed than H.R. 4585 in the insurance context, the model is consistent with the GLBA standard that state laws are preempted only if they are "inconsistent with" GLBA. State laws are not inconsistent with GLBA if the protections they afford are greater than GLBA protections. For our draft regulations, we have tried to track the concepts in GLBA for financial information while enhancing protections based on our model for individually identifiable health information.

V. Conclusion

We believe a national standard for the privacy of personal information is critical for both consumers and financial institutions. We also believe strongly that health information needs enhanced protections, and consumers should be assured that their personal health information will not be shared, sold or released without their specific consent.

We will continue to develop a uniform model regulation to meet the GLBA privacy mandate for insurance activities. Once our model is completed, the regulation must be adopted in each state or legislation must be enacted. Congressional action that could protect health privacy across the country could expedite this process and assure consumers that their personal health information will be protected regardless of where they live or which financial entity collects the information.

In light of the need to protect individually identifiable health information under the standards established in GLBA, we are glad you are addressing this issue. We appreciate your efforts, and in general we agree with the approach taken in H.R. 4585. We encourage you to please take this opportunity to address comprehensive privacy standards across the board for health information. The members of the NAIC would be happy to work with the Members of Congress in this area and willing to discuss and resolve any technical issues with Congressional staff. Thank you.

Section 6. Content of Disclosure Authorization Forms

Notwithstanding any other provision of law of this State, no insurance institution, agent or insurance support organization may utilize as its disclosure authorization form in connection with insurance transactions a form or statement which authorizes the disclosure of personal or privileged information about an individual to the insurance institution, agent or insurance support organization unless the form or statement:

A. Is written in plain language;

B. Is dated;

C. Specifies the types of persons authorized to disclose information about the individual;

D. Specifies the nature of the information authorized to be disclosed;

E. Names the insurance institution or agent and identifies by generic reference representatives of the insurance institution to whom the individual is authorizing information to be disclosed;

F. Specifies the purposes for which the information is collected;

G. Specifies the length of time such authorization shall remain valid, which shall be no longer than:

(1) In the case of authorizations signed for the purpose of collecting information in connection with an application for an insurance policy, a policy reinstatement or a request for change in policy benefits:

(a) Thirty (30) months from the date the authorization is signed if the application or request involves life, health or disability insurance;

(b) One (1) year from the date the authorization is signed if the application or request involves property or casualty insurance;

(2) In the case of authorizations signed for the purpose of collecting information in connection with a claim for benefits under an insurance policy,

(a) The term of coverage of the policy if the claim is for a health insurance benefit;

(b) The duration of the claim if the claim is not for a health insurance benefit; and

H. Advises the individual or a person authorized to act on behalf of the individual that the individual or the individual's authorized representative is entitled to receive a copy of the authorization form.

Drafting Note: The standard established by this section for disclosure authorization forms is intended to supersede any existing requirements a state may have adopted even if such requirements are more specific or applicable to particular authorizations such as medical information authorizations. This section is intended to be the exclusive statutory standard for all authorization forms utilized by insurance institutions, agents or insurance support organizations. This section does not preclude the inclusion of a disclosure authorization in an application form nor invalidate any disclosure authorizations in effect prior to the effective date of this Act. Nor does this section preclude an insurance institution, agent or insurance support organization from obtaining, in addition to its own authorization form which complies with this section, an additional authorization form required by the person from whom disclosure is sought.

Section 7. Investigative Consumer Reports

A. No insurance institution, agent or insurance support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement or a change in insurance benefits unless the insurance institution or agent informs the individual:

(1) That he or she may request to be interviewed in connection with the preparation of the investigative consumer report; and

(2) That upon a request pursuant to Section 8, he or she is entitled to receive a copy of the investigative consumer report.

B. If an investigative consumer report is to be prepared by an insurance institution or agent, the insurance institution or agent shall institute reasonable procedures to conduct a personal interview requested by an individual.

C. If an investigative consumer report is to be prepared by an insurance support organization, the insurance institution or agent desiring such report shall inform the insurance support organization whether a personal interview has been requested by the individual. The insurance support organization shall institute reasonable procedures to conduct such interviews, if requested.

Section 8. Access to Recorded Personal Information

A. If any individual, after proper identification, submits a written request to an insurance institution, agent or insurance support organization for access to recorded personal information about the individual which is reasonably described by the

individual and reasonably locatable and retrievable by the insurance institution, agent or insurance support organization, the insurance institution, agent or insurance support organization shall within thirty (30) business days from the date such request is received:

(1) Inform the individual of the nature and substance of such recorded personal information in writing, by telephone or by other oral communication, whichever the insurance institution, agent or insurance support organization prefers;

(2) Permit the individual to see and copy, in person, such recorded personal information pertaining to him or her or to obtain a copy of such recorded personal information by mail, whichever the individual prefers, unless such recorded personal information is in coded form, in which case an accurate translation in plain language shall be provided in writing;

(3) Disclose to the individual the identity, if recorded, of those persons to whom the insurance institution, agent or insurance support organization has disclosed such personal information within two (2) years prior to such request, and if the identity is not recorded, the names of those insurance institutions, agents, insurance support organizations or other persons to whom such information is normally disclosed; and

(4) Provide the individual with a summary of the procedures by which he or she may request correction, amendment or deletion of recorded personal information.

B. Any personal information provided pursuant to Subsection A above shall identify the source of the information if such source is an institutional source.

C. Medical-record information supplied by a medical care institution or medical professional and requested under Subsection A, together with the identity of the medical professional or medical care institution which provided such information, shall be supplied either directly to the individual or to a medical professional designated by the individual and licensed to provide medical care with respect to the condition to which the information relates, whichever the insurance institution, agent or insurance support organization prefers. If it elects to disclose the information to a medical professional designated by the individual, the insurance institution, agent or insurance support organization shall notify the individual, at the time of the disclosure, that it has provided the information to the medical professional.

D. Except for personal information provided under Section 10, an insurance institution, agent or insurance support organization may charge a reasonable fee to cover the costs incurred in providing a copy of recorded personal information to individuals.

E. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf. With respect to the copying and disclosure of recorded personal information pursuant to a request under Subsection A, an insurance institution, agent or insurance support organization may make arrangements with an insurance support organization or a consumer reporting agency to copy and disclose recorded personal information on its behalf.

F. The rights granted to individuals in this section shall extend to all natural persons to the extent information about them is collected and maintained by an insurance institution, agent or insurance support organization in connection with an insurance transaction. The rights granted to all natural persons by this subsection shall not extend to information about them that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving them.

G. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

Section 9. Correction, Amendment or Deletion of Recorded Personal Information

A. Within thirty (30) business days from the date of receipt of a written request from an individual to correct, amend or delete any recorded personal information about the individual within its possession, an insurance institution, agent or insurance support organization shall either:

(1) Correct, amend or delete the portion of the recorded personal information in dispute; or

(2) Notify the individual of:

(a) Its refusal to make such correction, amendment or deletion;

(b) The reasons for the refusal, and

(c) The individual's right to file a statement as provided in Subsection C.

B. If the insurance institution, agent or insurance support organization corrects, amends or deletes recorded personal information in accordance with Subsection A(1) above, the insurance institution, agent or insurance support organization shall so notify the individual in writing and furnish the correction, amendment or fact of deletion to:

(1) Any person specifically designated by the individual who may have, within the preceding two (2) years, received such recorded personal information;

(2) Any insurance support organization whose primary source of personal information is insurance institutions if the insurance support organization has systematically received such recorded personal information from the insurance institution within the preceding seven (7) years; provided, however, that the correction, amendment or fact of deletion need not be furnished if the insurance support organization no longer maintains recorded personal information about the individual; and

(3) Any insurance support organization that furnished the personal information that has been corrected, amended or deleted.

C. Whenever an individual disagrees with an insurance institution's, agent's or insurance support organization's refusal to correct, amend or delete recorded personal information, the individual shall be permitted to file with the insurance institution, agent or insurance support organization:

(1) A concise statement setting forth what the individual thinks is the correct, relevant or fair information; and

(2) A concise statement of the reasons why the individual disagrees with the insurance institution's, agent's or insurance support organization's refusal to correct, amend or delete recorded personal information.

D. In the event an individual files either statement as described in Subsection C above, the insurance institution, agent or insurance support organizations shall:

(1) File the statement with the disputed personal information and provide a means by which anyone reviewing the disputed personal information will be made aware of the individual's statement and have access to it; and

(2) In any subsequent disclosure by the insurance institution, agent or support organization of the recorded personal information that is the subject of disagreement, clearly identify the matter or matters in dispute and provide the individual's statement along with the recorded personal information being disclosed; and

(3) Furnish the statement to the persons and in the manner specified in Subsection B above.

E. The rights granted to individuals in this section shall extend to all natural persons to the extent information about them is collected and maintained by an insurance institution, agent or insurance support organization in connection with an insurance

transaction. The rights granted to all natural persons by this subsection shall not extend to information about them that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving them.

F. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent that this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

Section 10. Reasons for Adverse Underwriting Decisions

A. In the event of an adverse underwriting decision the insurance institution or agent responsible for the decision shall:

(1) Either provide the applicant, policyholder or individual proposed for coverage with the specific reason or reasons for the adverse underwriting decision in writing or advise such person that upon written request he or she may receive the specific reason or reasons in writing; and

(2) Provide the applicant, policyholder or individual proposed for coverage with a summary of the rights established under Subsection B and Sections 8 and 9 of this Act.

B. Upon receipt of a written request within ninety (90) business days from the date of the mailing of notice or other communication of an adverse underwriting decision to an applicant, policyholder or individual proposed for coverage, the insurance institution or agent shall furnish to such person within twenty-one (21) business days from the date of receipt of such written request:

(1) The specific reason or reasons for the adverse underwriting decision, in writing, if such information was not initially furnished in writing pursuant to Subsection A(1);

(2) The specific items of personal and privileged information that support those reasons; provided, however:

(a) The insurance institution or agent shall not be required to furnish specific items of privileged information if it has a reasonable suspicion, based upon specific information available for review by the Commissioner, that the applicant, policyholder or individual proposed for coverage has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, and

(b) Specific items of medical-record information supplied by a medical care institution or medical professional shall be disclosed either directly to the individual about whom the information relates or to a medical professional designated by the individual and licensed to provide medical care with respect to the condition to which the information relates, whichever the insurance institution or agent prefers, and

Drafting Note: The exception in Section 10B(2)(a) to the obligation of an insurance institution or agent to furnish the specific items of personal and privileged information that support the reasons for an adverse underwriting decision extends only to information about criminal activity, fraud, material misrepresentation or material nondisclosure that is privileged information and not to all information.

(3) The names and addresses of the institutional sources that supplied the specific items of information pursuant to Subsection B(2); provided, however, that the identity of any medical professional or medical care institution shall be disclosed either directly to the individual or to the designated medical professional, whichever the insurance institution or agent prefers.

C. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf.

D. When an adverse underwriting decision results solely from an oral request or inquiry, the explanation of reasons and summary of rights required by Subsection A may be given orally.

Section 11. Information Concerning Previous Adverse Underwriting Decisions

No insurance institution, agent or insurance support organization may seek information in connection with an insurance transaction concerning:

A. Any previous adverse underwriting decision experienced by an individual; or

B. Any previous insurance coverage obtained by an individual through a residual market mechanism,

unless such inquiry also requests the reasons for any previous adverse underwriting decision or the reasons why insurance coverage was previously obtained through a residual market mechanism.

Section 12. Previous Adverse Underwriting Decisions

No insurance institution or agent may base an adverse underwriting decision in whole or in part:

A. On the fact of a previous adverse underwriting decision or on the fact that an individual previously obtained insurance coverage through a residual market mechanism; provided, however, an insurance institution or agent may base an adverse underwriting decision on further information obtained from an insurance institution or agent responsible for a previous adverse underwriting decision;

B. On personal information received from an insurance support organization whose primary source of information is insurance institutions; provided, however, an insurance institution or agent may base an adverse underwriting decision on further personal information obtained as a result of information received from such insurance support organization.

Section 13. Disclosure Limitations and Conditions

An insurance institution, agent or insurance support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:

A. With the written authorization of the individual, provided:

(1) If such authorization is submitted by another insurance institution, agent or insurance support organization, the authorization meets the requirements of Section 6 of this Act; or

(2) If such authorization is submitted by a person other than an insurance institution, agent or insurance support organization, the authorization is:

(a) Dated;

(b) Signed by the individual; and

(c) Obtained one (1) year or less prior to the date a disclosure is sought pursuant to this subsection; or

B. To a person other than an insurance institution, agent or insurance support organization, provided such disclosure is reasonably necessary:

(1) To enable such person to perform a business, professional or insurance function for the disclosing insurance institution, agent or insurance support organization and such person agrees not to disclose the information further without the individual's written authorization unless the further disclosure:

(a) Would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

(b) Is reasonably necessary for such person to perform its function for the disclosing insurance institution, agent or insurance support organization; or

(2) To enable such person to provide information to the disclosing insurance institution, agent or insurance support organization for the purpose of:

(a) Determining an individual's eligibility for an insurance benefit or payment; or

(b) Detecting or preventing criminal activity, fraud, material misrepresentation or material nondisclosure in connection with an insurance transaction; or

C. To an insurance institution, agent, insurance support organization, or self-insurer, provided the information disclosed is limited to that which is reasonably necessary:

(1) To detect or prevent criminal activity, fraud, material misrepresentation or material nondisclosure in connection with insurance transactions; or

(2) For either the disclosing or receiving insurance institution, agent or insurance support organization to perform its function in connection with an insurance transaction involving the individual; or

D. To a medical care institution or medical professional for the purpose of:

(1) Verifying insurance coverage or benefits;

(2) Informing an individual of a medical problem of which the individual may not be aware; or

(3) Conducting an operations or services audit to verify the individuals treated by the medical professional or at the medical care institution;

provided only such information is disclosed as is reasonably necessary to accomplish the foregoing purposes; or

E. To an insurance regulatory authority; or

F. To a law enforcement or other governmental authority:

(1) To protect the interests of the insurance institution, agent or insurance support organization in preventing or prosecuting the perpetration of fraud upon it; or

(2) If the insurance institution, agent or insurance support organization reasonably believes that illegal activities have been conducted by the individual; or

G. Otherwise permitted or required by law; or

H. In response to a facially valid administrative or judicial order, including a search warrant or subpoena; or

I. Made for the purpose of conducting actuarial or research studies, provided:

(1) No individual may be identified in any actuarial or research report;

(2) Materials allowing the individual to be identified are returned or destroyed as soon as they are no longer needed; and

(3) The actuarial or research organization agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

J. To a party or representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the insurance institution, agent or insurance support organization, provided:

(1) Prior to the consummation of the sale, transfer, merger or consolidation only such information is disclosed as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger or consolidation; and

(2) The recipient agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

K. To a person whose only use of such information will be in connection with the marketing of a product or service, provided:

(1) No medical record information, privileged information or personal information relating to an individual's character, personal habits, mode of living or general reputation is disclosed, and no classification derived from such information is disclosed;

(2) The individual has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed; and

(3) The person receiving such information agrees not to use it except in connection with the marketing of a product or service; or

L. To an affiliate whose only use of the information will be in connection with an audit of the insurance institution or agent or the marketing of an insurance product or service, provided the affiliate agrees not to disclose the information for any other purpose or to unaffiliated persons; or

M. By a consumer reporting agency, provided the disclosure is to a person other than an insurance institution or agent; or

N. To a group policyholder for the purpose of reporting claims experience or conducting an audit of the insurance institution's or agent's operations or services, provided the information disclosed is reasonably necessary for the group policyholder to conduct the review or audit; or

O. To a professional peer review organization for the purpose of reviewing the service or conduct of a medical care institution or medical professional; or

P. To a governmental authority for the purpose of determining the individual's eligibility for health benefits for which the governmental authority may be liable; or

Q. To a certificateholder or policyholder for the purpose of providing information regarding the status of an insurance transaction; or

R. To a lienholder, mortgagee, assignee, lessor or other person shown on the records of an insurance institution or agent as having a legal or beneficial interest in a policy of insurance, provided that:

(1) No medical record information is disclosed unless the disclosure would otherwise be permitted by this section; and

(2) The information disclosed is limited to that which is reasonably necessary to permit such person to protect its interests in such policy.

Section 14. Power of Commissioner

A. The Commissioner shall have power to examine and investigate into the affairs of every insurance institution or agent doing business in this State to determine whether the insurance institution or agent has been or is engaged in any conduct in violation of this Act.

B. The Commissioner shall have the power to examine and investigate into the affairs of every insurance support organization acting on behalf of an insurance institution or agent which either transacts business in this State or transacts business outside

this State that has an effect on a person residing in this State in order to determine whether such insurance support organization has been or is engaged in any conduct in violation of this Act.

Section 15. Hearings, Witnesses, Appearances, Production of Books and Service of Process

A. Whenever the Commissioner has reason to believe that an insurance institution, agent or insurance support organization has been or is engaged in conduct in this State which violates this Act, or if the Commissioner believes that an insurance support organization has been or is engaged in conduct outside this State which has an effect on a person residing in this State and which violates this Act, the Commissioner shall issue and serve upon such insurance institution, agent or insurance support organization a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.

B. At the time and place fixed for such hearing the insurance institution, agent or insurance support organization charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the Commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.

C. At any hearing conducted pursuant to this section the Commissioner may administer oaths, examine and cross-examine witnesses and receive oral and documentary evidence. The Commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents which are relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the Commissioner. If no stenographic record is made and if judicial review is sought, the Commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this State.

D. Statements of charges, notices, orders and other processes of the Commissioner under this Act may be served by anyone duly authorized to act on behalf of the Commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered mail. A copy of the statement of charges, notice, order or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service, or return postcard receipt in the case of registered mail, shall be sufficient proof of service.

Section 16. Service of Process - Insurance Support Organizations

For the purpose of this Act, an insurance support organization transacting business outside this State which has an effect on a person residing in this State shall be deemed to have appointed the Commissioner to accept service of process on its behalf; provided the Commissioner causes a copy of such service to be mailed forthwith by registered mail to the insurance support organization at its last known principal place of business. The return postcard receipt for such mailing shall be sufficient proof that the same was properly mailed by the Commissioner.

Section 17. Cease and Desist Orders and Reports

A. If, after a hearing pursuant to Section 15, the Commissioner determines that the insurance institution, agent or insurance support organization charged has engaged in conduct or practices in violation of this Act, the Commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such insurance institution, agent or insurance support organization a copy of such findings and an order requiring such insurance institution, agent or insurance support organization to cease and desist from the conduct or practices constituting a violation of this Act.

B. If, after a hearing pursuant to Section 15, the Commissioner determines that the insurance institution, agent or insurance support organization charged has not engaged in conduct or practices in violation of this Act, the Commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurance institution, agent or insurance support organization charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.

C. Until the expiration of the time allowed under Section 19 of this Act for filing a petition for review or until such petition is actually filed, whichever occurs first, the Commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed under Section 19 of this Act for filing a petition for review, if no such petition has been duly filed, the Commissioner may, after notice and opportunity for hearing, alter, modify or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

Section 18. Penalties

A. In any case where a hearing pursuant to Section 15 results in the finding of a knowing violation of this Act, the Commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section 17, order payment of a monetary penalty of not more than [$500] for each violation but not to exceed [$10,000] in the aggregate for multiple violations.

B. Any person who violates a cease and desist order of the Commissioner under Section 17 of this Act may, after notice and hearing and upon order of the Commissioner, be

subject to one or more of the following penalties, at the discretion of the Commissioner:

(1) A monetary fine of not more than [$10,000] for each violation;

(2) A monetary fine of not more than [$50,000] if the Commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or

(3) Suspension or revocation of an insurance institution's or agent's license.

Section 19. Judicial Review of Orders and Reports

A. Any person subject to an order of the Commissioner under Section 17 or Section 18 or any person whose rights under this Act were allegedly violated may obtain a review of any order or report of the Commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the Commissioner be set aside. A copy of such petition shall be simultaneously served upon the Commissioner, who shall forthwith certify and file in such court a transcript of the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and transcript the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming or reversing any order or report of the Commissioner, in whole or in part. The findings of the Commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.

B. To the extent an order or report of the Commissioner is affirmed, the Court shall issue its own order commanding obedience to the terms of the order or report of the Commissioner. If any party affected by an order or report of the Commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the Commissioner in such manner and upon such terms and conditions as the court may deem proper. The Commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.

C. An order or report issued by the Commissioner under Section 17 or 18 shall become final:

(1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the Commissioner may modify or set aside an order or report to the extent provided in Section 17C; or

(2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the Commissioner be affirmed or the petition for review dismissed.

D. No order or report of the Commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any person affected by such order or report from any liability under any law of this State.

Section 20. Individual Remedies

A. If any insurance institution, agent or insurance support organization fails to comply with Section 8, 9 or 10 of this Act with respect to the rights granted under those sections, any person whose rights are violated may apply to the [insert title] Court of this State, or any other court of competent jurisdiction, for appropriate equitable relief.

B. An insurance institution, agent or insurance support organization which discloses information in violation of Section 13 of this Act shall be liable for damages sustained by the individual about whom the information relates; provided, however, that no individual shall be entitled to a monetary award which exceeds the actual damages sustained by the individual as a result of a violation of Section 13 of this Act.

C. In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.

D. An action under this section must be brought within two (2) years from the date the alleged violation is or should have been discovered.

E. Except as specifically provided in this section, there shall be no remedy or recovery available to individuals, in law or in equity, for occurrences constituting a violation of any provisions of this Act.

Section 21. Immunity

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurance institution, agent or insurance support organization; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

Section 22. Obtaining Information Under False Pretenses

Any person who knowingly and willfully obtains information about an individual from an insurance institution, agent or insurance support organization under false pretenses shall be fined not more than [$10,000] or imprisoned for not more than one year, or both.

Section 23. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 24. Effective Date

A. This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].

B. The rights granted under Sections 8, 9 and 13 of this Act shall take effect on [insert effective date] regardless of the date of the collection or receipt of the information which is the subject of such sections.

Legislative History (all references are to the Proceedings of the NAIC).

1980 Proc. I 34, 38, 281, 319, 320-335 (adopted).
1981 Proc. I 47, 51, 255, 259, 290-313 (revised and reprinted).
1982 Proc. I 19, 27, 155, 198 (amended).

Attachment A

NAIC INSURANCE INFORMATION AND PRIVACY PROTECTION MODEL ACT

Table of Contents

Preamble

The purpose of this Act is to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance support organizations; to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy; to limit the disclosure of information collected in connection with insurance transactions; and to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.

Section 1. Scope

A. The obligations by this Act shall apply to those insurance institutions, agents or insurance support organizations which, on or after the effective date of this Act:

(1) In the case of life, health and disability insurance:

(a) Collect, receive or maintain information in connection with insurance transactions which pertains to natural persons who are residents of this State, or

(b) Engage in insurance transactions with applicants, individuals or policyholders who are residents of this State, and

(2) In the case of property or casualty insurance:

(a) Collect, receive or maintain information in connection with insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this State, or

(b) Engage in insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this State.

B. The rights granted by this Act shall extend to:

(1) In the case of life, health or disability insurance, the following persons who are residents of this State:

(a) Natural persons who are the subject of information collected, received or maintained in connection with insurance transactions, and

(b) Applicants, individuals or policyholders who engage in or seek to engage in insurance transactions, and

(2) In the case of property or casualty insurance, the following persons:

(a) Natural persons who are the subject of information collected, received or maintained in connection with insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this State, and

(b) Applicants, individuals or policyholders who engage in or seek to engage in insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this State.

C. For purposes of this section, a person shall be considered a resident of this State if the person's last known mailing address, as shown in the records of the insurance institution, agent or insurance support organization, is located in this State.

D. Notwithstanding Subsections A and B above, this Act shall not apply to information collected from the public records of a governmental authority and maintained by an insurance institution or its representatives for the purpose of insuring the title to real property located in this State.

Section 2. Definitions

As used in this Act:

A. "Adverse underwriting decision" means:

(1) Any of the following actions with respect to insurance transactions involving insurance coverage which is individually underwritten:

(a) A declination of insurance coverage;

(b) A termination of insurance coverage;

(c) Failure of an agent to apply for insurance coverage with a specific insurance institution which the agent represents and which is requested by an applicant;

(d) In the case of a property or casualty insurance coverage:

(i) Placement by an insurance institution or agent of a risk with a residual market mechanism, an unauthorized insurer or an insurance institution which specializes in substandard risks; or

(ii) The charging of a higher rate on the basis of information which differs from that which the applicant or policyholder furnished;

Drafting Note: The use of the term "substandard" in Section 2A(d)(i) is intended to apply to those insurance institutions whose rates and market orientation are directed at risks other than preferred or standard risks. To facilitate compliance with this Act, Commissioners should consider developing a list of insurance institutions operating in their state which specialize in substandard risks and make it known to insurance institutions and agents.

(e) In the case of a life, health or disability insurance coverage, an offer to insure at higher than standard rates.

(2) Notwithstanding Paragragh (1) above, the following actions shall not be considered adverse underwriting decisions but the insurance institution or agent responsible for their occurrence shall nevertheless provide the applicant or policyholder with the specific reason or reasons for their occurrence:

(a) The termination of an individual policy form on a class or statewide basis;

(b) A declination of insurance coverage solely because such coverage is not available on a class or statewide basis; or

(c) The rescission of a policy.

B. "Affiliate" or "affiliated" means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person.

C. "Agent" means [make reference here to every appropriate statutory category of producer, including brokers, authorized to do business in the State. This is necessary because in many states different types of producers, or producers for certain types of insurance institutions are referred to by specific statutory terms in the insurance code.]

D. "Applicant" means a person who seeks to contract for insurance coverage other than a person seeking group insurance that is not individually underwritten.

E. "Commissioner" means [insert the appropriate title and statutory reference for the principal insurance regulatory official of the State.]

F. "Consumer report" means a written, oral or other communication of information bearing on a natural person's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used in connection with an insurance transaction.

G. "Consumer reporting agency" means a person who:

(1) Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;

(2) Obtains information primarily from sources other than insurance institutions; and

(3) Furnishes consumer reports to other persons.

H. "Control," including the terms "controlled by" or "under common control with," means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise, unless the power is the result of an official position with or corporate office held by the person.

I. "Declination of insurance coverage" means a denial, in whole or in part, by an insurance institution or agent of requested insurance coverage.

J. "Individual" means a natural person who:

(1) In the case of property or casualty insurance, is a past, present or proposed named insured or certificateholder;

(2) In the case of life, health or disability insurance, is a past, present or proposed principal insured or certificateholder;

(3) Is a past, present or proposed policyowner;

(4) Is a past or present applicant;

(5) Is a past or present claimant; or

(6) Derived, derives or is proposed to derive insurance coverage under an insurance policy or certificate subject to this Act.

K. "Institutional source" means any person or governmental entity that provides information about an individual to an agent, insurance institution or insurance support organization, other than:

(1) An agent;

(2) The individual who is the subject of the information; or

(3) A natural person acting in a personal capacity rather than in a business or professional capacity.

L. "Insurance institution" means any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's insurer, fraternal benefit society or other person engaged in the business of insurance, including health maintenance organizations, medical service plans and hospital service plans as defined in [insert the applicable section of the State insurance code which defines health maintenance organizations or medical or hospital service plans.] "Insurance institution" shall not include agents or insurance support organizations.

M. "Insurance support organization" means:

(1) Any person who regularly engages, in whole or in part, in the practice of assembling or collecting information about natural persons for the primary purpose of providing the information to an insurance institution or agent for insurance transactions, including:

(a) The furnishing of consumer reports or investigative consumer reports to an insurance institution or agent for use in connection with an insurance transaction, or

(b) The collection of personal information from insurance institutions, agents or other insurance support organizations for the purpose of detecting or preventing fraud, material misrepresentation or material nondisclosure in connection with insurance underwriting or insurance claim activity.

(2) Notwithstanding Paragraph (1) above, the following persons shall not be considered "insurance support organizations" for purposes of this Act: agents, government institutions, insurance institutions, medical care institutions and medical professionals.

N. "Insurance transaction" means any transaction involving insurance primarily for personal, family or household needs rather than business or professional needs which entails:

(1) The determination of an individual's eligibility for an insurance coverage, benefit or payment; or

(2) The servicing of an insurance application, policy, contract or certificate.

O. "Investigative consumer report" means a consumer report or portion thereof in which information about a natural person's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with the person's neighbors, friends, associates, acquaintances or others who may have knowledge concerning such items of information.

P. "Medical-care institution" means any facility or institution that is licensed to provide health care services to natural persons, including but not limited to: health-maintenance organizations home-health agencies, hospitals, medical clinics, public health agencies, rehabilitation agencies and skilled nursing facilities.

Q. "Medical professional" means any person licensed or certified to provide health care services to natural persons, including but not limited to, a chiropractor, clinical dietician, clinical psychologist, dentist, nurse, occupational therapist, optometrist,

pharmacist, physical therapist, physician, podiatrist, psychiatric social worker or speech therapist.

R. "Medical record information" means personal information which:

(1) Relates to an individual's physical or mental condition, medical history or medical treatment; and

(2) Is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

S. "Person" means any natural person, corporation, association, partnership or other legal entity.

T. "Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics. "Personal information" includes an individual's name and address and "medical record information" but does not include "privileged information".

U. "Policyholder" means any person who:

(1) In the case of individual property or casualty insurance, is a present named insured;

(2) In the case of individual life, health or disability insurance, is a present policyowner; or

(3) In the case of group insurance which is individually underwritten, is a present group certificateholder.

V. "Pretext interview" means an interview whereby a person, in an attempt to obtain information about a natural person, performs one or more of the following acts:

(1) Pretends to be someone he or she is not;

(2) Pretends to represent a person he or she is not in fact representing;

(3) Misrepresents the true purpose of the interview; or

(4) Refuses to identify himself or herself upon request.

W. "Privileged information" means any individually identifiable information that:

(1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual; and

(2) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual;

provided, however, information otherwise meeting the requirements of this subsection shall nevertheless be considered "personal information" under this Act if it is disclosed in violation of Section 13 of this Act.

Drafting Note: The phrase "in reasonable anticipation of a claim" contemplates that the insurance institution has knowledge of a loss but has not received formal notice of the claim.

X. "Residual market mechanism" means an association, organization or other entity defined or described in Sections(s) [insert those sections of the State insurance code authorizing the establishment of a FAIR Plan, assigned risk plan, reinsurance facility, joint underwriting association, etc.]

Drafting Note: Those states having a reinsurance facility may want to exclude it from this definition if the state's policy is not to disclose to insureds the fact that they have been reinsured in the facility.

Y. "Termination of insurance coverage" or "termination of an insurance policy" means either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than the failure to pay a premium as required by the policy.

Z. "Unauthorized insurer" means an insurance institution that has not been granted a certificate of authority by the Commissioner to transact the business of insurance in this state.

Drafting Note: Each state must make sure that this definition is consistent with its surplus lines laws.

Section 3. Pretext Interviews

No insurance institution, agent or insurance support organization shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, a pretext interview may be undertaken to obtain information from a person or institution that does not have a generally or statutorily recognized privileged relationship with the person about whom the information relates for the purpose of investigating a claim where, based upon specific information available for review by the Commissioner, there is a reasonable basis for suspecting criminal activity, fraud, material misrepresentation or material nondisclosure in connection with the claim.

Drafting Note: Some states may desire to eliminate the exception in this section and thereby prohibit pretext interviews in all instances. Other states may desire to broaden the exception so that pretext interviews can be utilized in underwriting and rating situations as well as claim situations. States may either expand or limit the prohibition against pretext interviews suggested in this section to accommodate their individual needs and circumstances. Deviation from the standard developed here should not seriously undermine efforts to achieve uniform rules for insurance information practices throughout the various states.

Section 4. Notice of Insurance Information Practices

A. An insurance institution or agent shall provide a notice of information practices to all applicants or policyholders in connection with insurance transactions as provided below:

(1) In the case of an application for insurance, a notice shall be provided no later than:

(a) At the time of the delivery of the insurance policy or certificate when personal information is collected only from the applicant or from public records; or

(b) At the time the collection of personal information is initiated when personal information is collected from a source other than the applicant or public records;

(2) In the case of a policy renewal, a notice shall be provided no later than the policy renewal date, except that no notice shall be required in connection with a policy renewal if:

(a) Personal information is collected only from the policyholder or from public records; or

(b) A notice meeting the requirements of this section has been given within the previous twenty-four (24) months; or

(3) In the case of a policy reinstatement or change in insurance benefits, a notice shall be provided no later than the time a request for a policy reinstatement or change in insurance benefits is received by the insurance institution, except that no notice shall be required if personal information is collected only from the policyholder or from public records.

B. The notice required by Subsection A above shall be in writing and shall state:

(1) Whether personal information may be collected from persons other than the individual or individuals proposed for coverage;

(2) The types of personal information that may be collected and the types of sources and investigative techniques that may be used to collect such information;

(3) The types of disclosures identified in subsections B, C, D, E, F, I, K, L and N of Section 13 of this Act and the circumstances under which such disclosures may be made without prior authorization; provided, however, only those circumstances need be described which occur with such frequency as to indicate a general business practice;

(4) A description of the rights established under Sections 8 and 9 of this Act and the manner in which such rights may be exercised; and

(5) That information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

C. In lieu of the notice prescribed in Subsection B, the insurance institution or agent may provide an abbreviated notice informing the applicant or policyholder that:

(1) Personal information may be collected from persons other than the individual or individuals proposed for coverage;

(2) Such information as well as other personal or privileged information subsequently collected by the insurance institution or agent may in certain circumstances be disclosed to third parties without authorization;

(3) A right of access and correction exists with respect to all personal information collected; and

(4) The notice prescribed in Subsection B will be furnished to the applicant or policyholder upon request.

D. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf.

Drafting Note: If permitted under Section 4A, an insurance institution or agent may include the notice in the insurance policy or certificate.

Section 5. Marketing and Research Surveys

An insurance institution or agent shall clearly specify those questions designed to obtain information solely for marketing or research purposes from an individual in connection with an insurance transaction.

Attachment B

HEALTH INFORMATION PRIVACY MODEL ACT

Table of Contents

Section 1. Title

This Act may be known and shall be cited as the Health Information Privacy Act.

Section 2. Purpose

The purpose of this Act is to set standards to protect health information from unauthorized collection, use and disclosure by requiring carriers to establish procedures for the treatment of all health information.

Section 3. Definitions

As used in this Act:

A. "Carrier" means a person or entity required to be licensed or authorized by the commissioner to assume risk, including but not limited to an insurer, a hospital, medical or health service corporation, a health maintenance organization, a provider sponsored organization, a multiple employer welfare arrangement, a self-insured group fund or a workers' compensation self-insurer. Carrier does not include a non-risk-bearing regulated insurance entity, such as a producer, agency or administrator.

Drafting Note: Some entities that collect, use or disclose protected health information may not be subject to the jurisdiction of the insurance commissioner, but may be subject to the jurisdiction of another state agency, such as the Department of Labor or the Department of Health. States may want to ensure fair and equitable regulation of all entities that collect, use or disclose protected health information by making parallel amendments to other appropriate state laws, such as workers' compensation laws.

B. "Commissioner" means the insurance commissioner of this state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health carriers, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

C. "Covered person" means a policyholder, subscriber, enrollee, beneficiary, insured, certificateholder or other person covered by a policy, contract or agreement of insurance issued by a carrier.

D. "Disclose" means to release, transfer, or otherwise divulge protected health information to any person other than to the individual who is the subject of the protected health information.

E. "Facility" means an institution providing health care services or a health care setting, including but not limited to hospitals and other licensed inpatient centers, ambulatory surgical or treatment centers, skilled nursing centers, residential treatment centers, diagnostic, laboratory and imaging centers, and rehabilitation and other therapeutic health settings.

F. "Health care" means:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, services, procedures, tests or counseling that:

(a) Relates to the physical, mental or behavioral condition of an individual; or

(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or

(2) Prescribing, dispensing, or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

G. "Health care professional" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law.

H. "Health care provider" or "provider" means a health care professional or facility.

I. "Health information" means any information or data, whether oral or recorded in any form or medium, and personal facts or information about events or relationships that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual or a member of the individual's family;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

J. "Insurance support organization" means a person that regularly engages, in whole or in part, in the practice of assembling or collecting information from carriers, agents or other insurance support organizations for the purpose of ratemaking or ratemaking-related functions, regulatory or legislative cost analysis, detecting or preventing fraud, material misrepresentation or material nondisclosure in connection with insurance underwriting or insurance claim activity. Persons that are not considered "insurance support organizations" for purposes of this Act are agents, government institutions, insurance institutions, medical care institutions and medical professionals.

Drafting Note: States may wish to include either separately or in the definition section, a definition of the term "insurance institution," from the NAIC Insurance Information and Privacy Protection Model Act. "Insurance institution" means any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's insurer, fraternal benefit society or other person engaged in the business of insurance, including health maintenance organizations, medical service plans and hospital service plans as defined in [insert applicable section of the State insurance code which defines health maintenance organization or medical or hospital service plans.]

K. "Person" means an individual, a corporation, a partnership, an association, a joint venture, a joint stock company, a trust, an unincorporated organization, any similar entity or a combination of the foregoing.

L. "Protected health information" means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

M. "Research" means the process of systematic investigation or inquiry including, but not limited to any of the following: the systematic development and testing of a hypothesis; and the systematic description, analysis and measurement of processes, behaviors and physical, social, political or medical phenomena.

N. "Research organization" means a person or organization, other than the carrier disclosing the protected health information, engaged in research.

O. (1) "Scientific, medical or public policy research" means research conducted to improve the effectiveness of:

(a) Determining medical causation, diagnosis and treatment;

(b) Public health; or

(c) The operations of the public or private health care, insurance or workers' compensation systems; and

(2) (a) The results of the research are intended for publication;

(b) The research findings are intended to be widely disseminated beyond the carrier and research organization so as to benefit the public good; and

(3) The scientific, medical or public policy research excludes all activities listed in Section 10H(1).

P. "Unauthorized" means a collection, use or disclosure of protected health information made by a carrier without the authorization of the subject of that protected health information or that is not in compliance with this Act, unless collection, use or disclosure without an authorization is permitted by this Act.

Section 4. Applicability and Scope

This Act applies to all carriers and governs the management of health information, including the collection, use, and disclosure of protected health information by carriers.

Section 5. Health Information Policies, Standards and Procedures

A. A carrier shall develop and implement written policies, standards and procedures for the management of health information, including policies, standards and procedures to guard against the unauthorized collection, use or disclosure of protected health information by the carrier which shall include:

(1) Limitation on access to health information by only those persons who need to use the health information in order to perform their jobs;

(2) Appropriate training for all employees;

(3) Disciplinary measures for violations of the health information policies, standards and procedures;

(4) Identification of the job titles and job descriptions of persons that are authorized to disclose protected health information;

(5) Procedures for authorizing and restricting the collection, use or disclosure of protected health information;

(6) Methods for exercising the right to access and amend protected health information as provided in Sections 7 and 8;

(7) Methods for handling, disclosing, storing and disposing of health information;

(8) Periodic monitoring of the employees' compliance with the carrier's policies, standards and procedures in a manner sufficient for the carrier to determine compliance with this Act and to enforce its policies, standards and procedures; and

(9) Methods for informing and allowing an individual who is the subject of protected health information to request specialized disclosure or nondisclosure of protected health information as required under Section 14.

B. (1) In any contractual arrangement between a carrier and a person other than a covered person or health care provider where the person collects or uses protected health information on behalf of the carrier or where the carrier discloses protected health information to the person a carrier shall:

(a) Require the person to have health information policies, standards and procedures that comply with the requirements of this Act; and

(b) Inform the person of its obligation to comply with any applicable state and federal statutory and regulatory requirements governing the collection, use or disclosure of protected health information.

(2) In any contractual arrangement between a carrier and a health care provider, a carrier shall require that the health care provider have health information privacy policies, standards and procedures.

(3) Notwithstanding Section 18, all contractual arrangements described in this subsection in effect on [insert effective date], shall comply with this Act no later than eighteen (18) months after [insert effective date] or the renewal date of the contract, whichever is earlier.

C. A carrier shall make the health information policies, standards and procedures developed pursuant to this section available for review by the commissioner.

Section 6. Notice of Health Information Policies, Standards and Procedures

A. A carrier shall draft a written notice of its health information policies, standards and procedures developed pursuant to Section 5, which shall be made available for review by the commissioner. The notice shall include:

(1) The collection, use and disclosure of protected health information prohibited and permitted by this Act;

(2) The procedures for authorizing and limiting disclosures of protected health information and for revoking authorizations;

(3) The procedures for accessing and amending protected health information; and

(4) The right of a covered person to review a copy of the carrier's health information policies, standards and procedures.

B. The carrier shall provide the notice to any person upon request, to covered persons at the time the policy is first delivered, and to all other individuals when requesting an authorization. If subsequent policies are issued to the same insured, no additional notices are required to be included when those subsequent policies are delivered.

Drafting Note: The language regarding subsequent policies is meant to clarify that notice does not need to be redelivered every time changes are made to the policy a carrier has with an existing policyholder. For example, notice need not be redelivered when an automobile is added to an automobile insurance policy.

Section 7. Right to Access Protected Health Information

A. Subject to the exceptions listed in Subsection B(3) of this section, an individual who is the subject of the protected health information has the right to examine or receive a copy of the protected health information that is in the possession of the carrier or a person acting on behalf of the carrier.

B. No later than twenty (20) working days after receipt of a written request for protected health information from an individual who is the subject of protected health information, a carrier shall do one of the following:

(1) Provide a copy of the protected health information requested to the individual or if providing a copy is not possible, permit the individual to examine the protected health information during regular business hours;

(2) Notify the individual that the carrier does not have the protected health information and, if known, inform the individual of the name and address of the person who has the protected health information requested or, if the carrier will be obtaining access to the requested protected health information, when the protected health information is expected to be available to the individual; or

(3) Deny the request in whole or in part if the carrier determines any of the following:

(a) Knowledge of the protected health information would reasonably be expected to identify a confidential source who provided the protected health information in conjunction with a lawfully conducted investigation, law enforcement investigation, or court proceeding;

(b) The protected health information was compiled in preparation for litigation, law enforcement or fraud investigation, quality assurance or peer review purposes;

(c) The protected health information is the original work product of the carrier, which would include but not be limited to interpretation, mental impressions, instructions and other original product of the carrier, its employees and agents;

(d) The requester is a party to a legal proceeding involving the carrier where the health condition of the requester is at issue. However, once a legal proceeding is resolved, the individual's right to access protected health information under this section and to amend protected health information under Section 8 shall be restored; or

(e) Disclosure of the protected health information to the individual who is the subject of the protected health information is otherwise prohibited by law.

C. If a request to examine or copy protected health information is denied in whole or in part under this section, the carrier shall notify the individual who is the subject of the protected health information of the reasons for the denial in writing. When the protected health information was compiled in preparation for litigation, law enforcement or fraud investigation, the carrier is not required to notify the individual of the reasons for the denial.

Drafting Note: When the information that has been requested is not subject to release, the carrier should inform the requester that all information required to be released under this Act has been released.

D. A carrier is not required to create a new record or reformulate an existing record in order to meet a request for protected health information.

E. The carrier may charge a reasonable fee for providing the protected health information requested and shall provide a detailed bill accounting for the charges. No charge shall be made for reproduction of protected health information requested for the purpose of supporting a claim, supporting an appeal or accessing any federal or state sponsored or operated health benefits program.

Section 8. Right to Amend Protected Health Information

A. An individual who is the subject of protected health information has the right to amend the protected health information to correct any inaccuracies.

B. Within thirty (30) working days after receipt of a written request from an individual who is the subject of protected health information to amend protected health information, a carrier shall act to verify the accuracy of protected health information identified as erroneous by the individual and shall do one of the following:

(1) Correct or amend (either by changing the information in question or adding additional information as provided by the individual), or delete the portion of the protected health information in dispute and notify the individual of the changes; or

(2) Notify the individual that the request has been denied, the reason for the denial, and that the individual may:

(a) Request that the health care provider who created the record in question amend the record. The carrier shall include the health care provider's name and address; or

(b) File a concise statement of what the individual believes to be the correct information and the reasons why the individual disagrees with the denial. The carrier shall retain this statement filed by the individual with the protected health information.

C. If the carrier corrects, amends or deletes the protected health information as requested pursuant to Subsection B(1), the carrier shall furnish the correction, amendment or deletion to:

(1) All persons who have received the protected health information that has been corrected, amended or deleted from the carrier within the preceding two (2) years;

(2) An insurance support organization whose primary source of protected health information is carriers, as long as the insurance support organization has systematically received protected health information from the carrier within the preceding seven (7) years. However, the correction, amendment or deletion need not be furnished if the insurance support organization no longer maintains the protected health information that has been corrected, amended or deleted; and

(3) Any person that furnished the protected health information that was amended pursuant to Subsection B(1).

D. If the individual who is the subject of the protected health information files a statement pursuant to Subsection B(2)(b), the carrier shall:

(1) Clearly identify the matter or matters in dispute and include the statement in any subsequent disclosure of the protected health information; and

(2) Furnish the statement to the persons described in Subsection C.

E. Nothing in this section shall require a carrier to alter, delete, erase or obliterate medical records provided to them by a health care provider.

F. Nothing in this section shall be construed to give a person access to protected health information covered by the exceptions listed in Section 7B(3).

Section 9. List of Disclosures of Protected Health Information

A. A carrier shall provide upon request, to an individual who is the subject of the protected health information, information regarding disclosure of that individual's protected health information that is sufficient to exercise the right to amend the information pursuant to Section 8. This information shall include the date, purpose, recipient and relevant authorization or basis for the disclosure. The carrier may charge a reasonable fee for providing the information regarding the disclosures of information.

B. A carrier shall maintain a system that is sufficient for the commissioner to determine that the carrier can produce a complete list of disclosures.

(1) For routine disclosures, a carrier shall be able to track when routine disclosures are made, to whom they are made and for what purpose they are made; and

(2) For all other disclosures, a carrier shall be able to identify the authorization or release form or provision of law allowing the receipt or disclosure of protected health information.

C. A carrier is not required to include in the information developed pursuant to Section 9A any disclosures of protected health information that were compiled in preparation for litigation, law enforcement or fraud investigation.

Section 10. Authorization for Collection, Use or Disclosure of Protected Health Information

A. A carrier shall not collect, use or disclose protected health information without a valid authorization from the subject of the protected health information, except as permitted by Section 11 of this Act or as permitted or required by law or court order. Authorization for the disclosure of protected health information may be obtained for any purpose, provided that the authorization meets the requirements of this section.

B. A carrier shall retain the authorization or a copy thereof in the record of the individual who is the subject of the protected health information.

C. A valid authorization shall be in writing and contain all the following:

(1) The identity of the individual who is the subject of the protected health information;

(2) A description of the types of protected health information to be collected, used or disclosed. If the authorization is in support of an application for coverage where tests, including genetic tests, and examinations are to be performed in conjunction with underwriting the application, the authorization shall include a description of the types of tests or examinations to be performed and shall be accompanied by a statement that the tested individual may choose whether to receive the results of any laboratory tests or medical examinations performed. In cases where the authorization is other than in support of an application for coverage, and tests, including genetic tests, and examinations are to be performed, an individual may choose whether to receive the results of any laboratory tests or medical examinations performed and obtain, upon request, a detailed list of laboratory tests or medical examinations to be performed before tests or examinations are administered;

(3) A general description of the sources from which protected health information will be collected;

(4) The name and address of the person to whom the protected health information is to be disclosed, except that an authorization provided to a carrier for collection of protected health information to support insurance functions listed in Section 10H may generally describe the persons to whom protected health information may be disclosed;

(5) The purpose of the authorization, including the reason for the collection, the intended use of the protected health information, and the scope of any disclosures that may be made in carrying out the purpose for which the authorization is requested, provided those disclosures are not otherwise prohibited by law;

(6) The signature of the individual who is the subject of the protected health information or the individual who is legally empowered to grant authority and the date signed; and

(7) A statement that the individual who is the subject of the protected health information may revoke the authorization at any time, except as provided in Subsection G and subject to the rights of any person that acted in reliance on the authorization prior to revocation.

D. An authorization shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twelve (12) months, except an authorization signed for one of the following purposes:

(1) For the collection of protected health information to support insurance functions listed in Section 10H, in which event the authorization shall remain valid during the entire term of the policy or as long as necessary for the carrier to meet its obligations under the policy or as otherwise required by law;

(2) To support an application for, a reinstatement of, or a change in benefits under a life insurance policy, in which event the authorization shall expire in thirty (30) months or whenever the application is denied, whichever occurs first; or

(3) To support or facilitate ongoing management of a chronic condition or illness or rehabilitation from an injury.

E. A carrier shall obtain a separate authorization to disclose protected health information to an individual's employer, including the employer's designated risk manager, unless:

(1) The protected health information is disclosed pursuant to the employer's workers' compensation program, to the extent necessary for the performance of the employer's and carrier's rights and duties under state laws governing workers' compensation;

(2) The protected health information is disclosed pursuant to the employer's administration of a health and welfare benefit plan; or

(3) The protected health information is necessary to the administration of claims pursuant to a commercial lines policy.

F. A carrier shall obtain a separate authorization to collect, use or disclose protected health information if the purpose of the collection, use or disclosure under

Subsection C(5) is for the marketing of services or goods, or for other commercial gain. The purpose of the collection, use or disclosure shall appear as a separate paragraph in bold type no smaller than twelve (12) point. The purpose shall be stated in clear and simple terms. The request for authorization shall specify that the authorization shall remain valid for no more than twelve (12) months and may be revoked at any time. The request for authorization shall state that the terms and conditions of all insurance policies will not be affected in any way by a refusal to give authorization. A separate authorization is not required if the use or disclosure is internal or to an affiliate and the only use of the information will be in connection with the marketing of an insurance product, provided the affiliate agrees not to disclose the information for any other purpose or to unaffiliated persons. With respect to insurance products, the individual shall be given an opportunity to indicate that he or she does not want protected health information used for marketing purposes and shall have given no indication that he or she does not want protected health information used for these purposes.

G. An individual who is the subject of protected health information may revoke an authorization at any time, subject to the rights of any person who acted in reliance on the authorization prior to notice of revocation. A revocation of an authorization shall be in writing, dated and signed. A revocation of an authorization shall be retained by the carrier in the record of the individual who is the subject of the protected health information. A carrier shall give prompt notice of the revocation to all persons to whom the carrier has disclosed protected health information in reliance on the initial authorization.

H. (1) A carrier that has collected protected health information pursuant to a valid authorization in accordance with this Act, may use and disclose the protected health information to a person acting on behalf of or at the direction of the carrier for the performance of the carrier's insurance functions: claims administration, claims adjustment and management, fraud investigation, underwriting, loss control, rate-making functions, reinsurance, risk management, case management, disease management, quality assessment, quality improvement, provider credentialing verification, utilization review, peer review activities, grievance procedures, and internal administration of compliance, managerial, information systems, and policyholder service functions. Additional insurance functions may be allowed with the prior approval of the commissioner.

(2) The protected health information shall not be used or disclosed for any purpose other than in the performance of the carrier's insurance functions, except as otherwise permitted in this Act.

I. An authorization to collect, use or disclose protected health information pursuant to this Act or a production of protected health information pursuant to a court order shall not be construed to constitute a waiver of any other privacy right provided to an individual who is the subject of protected health information by other federal or state laws, common law, or rules of evidence.

J. A person who receives protected health information from a carrier shall not use the protected health information for any purpose other than the lawful purpose for which it was disclosed.

K. Nothing in this Act requires a carrier to provide a benefit or commence or continue payment of a claim in the absence of protected health information to support or deny the benefit or claim.

L. A carrier that has collected protected health information prior to the effective date of this Act is not required to obtain an authorization for the information; however the information may only be used or disclosed in accordance with this Act after the effective date.

Drafting Note: States with laws addressing the electronic transmission of information may want to specifically authorize the use of electronic authorizations in this section.

Section 11. Collection, Use and Disclosure of Protected Health Information Without Authorization: Generally

A. A carrier may engage in the following activities with regard to protected health information without authorization in the following circumstances or as otherwise permitted by law:

(1) Collect protected health information from or disclose protected health information to a carrier, provided that the carrier that is receiving the information:

(a) Is investigating, evaluating, adjusting or settling a claim involving the individual who is the subject of the protected health information; or

(b) Has become or is considering becoming liable under a policy insuring the individual who is the subject of the protected health information as a result of a merger, acquisition or other assumption of such liability;

(2) Collect, use or disclose protected health information to the extent necessary to investigate, evaluate, subrogate or settle third party claims, provided that the claimant is the subject of the protected health information and the protected health information is used for no other purpose without a valid authorization or the use is otherwise permitted under federal or state law;

(3) (a) Collect, use or disclose protected health information to or from an insurance support organization provided that:

(i) The insurance support organization has in place health information policies, standards and procedures to ensure compliance with the requirements of this Act; and

(ii) The protected health information is used only to perform the insurance functions of claims settlement, detection and prevention of fraud, or detection and prevention of material misrepresentation or material nondisclosure; or

(iii) The protected health information is collected and used internally only to perform the insurance functions of ratemaking and ratemaking-related functions or regulatory or legislative cost analysis; and

(b) Additional insurance functions may be added to Subparagraphs (3)(a)(ii) and (iii) with prior approval of the commissioner;

(4) If the protected health information is necessary to provide ongoing health care treatment, and if the disclosure has not been limited or prohibited by the covered person who is the subject of the information, collect protected health information from or disclose protected health information to:

(a) A health care provider, employed by the carrier, who is furnishing health care to a covered person;

(b) A health care provider with whom the carrier contracts to provide health care services to covered persons; or

(c) A referring health care provider who continues to furnish health care to a covered person;

(5) Disclose protected health information to a person engaged in the assessment, evaluation or investigation of the quality of health care furnished by a provider pursuant to statutory or regulatory standards or pursuant to the requirements of a private or public program authorized to provide for the payment of health care;

(6) Subject to the limits of Section 14A, disclose protected health information to reveal a covered person's presence in a facility owned by the carrier and the covered person's general health condition, provided that the disclosure is limited to directory information, unless the covered person has restricted that disclosure or the disclosure is otherwise prohibited by law. For the purposes of this paragraph, directory information means information about the presence or general health condition of a particular covered person who is a patient or is receiving emergency health care in a health care facility. General health condition means the covered person's general health condition or status described as "critical," "poor," "fair," "good," "excellent," or in terms that denote similar conditions;

(7) Collect, use or disclose protected health information when the protected health information is necessary to the performance of the carrier's obligations under any workers' compensation law or contract;

(8) Collect protected health information from or disclose protected health information to a reinsurer, stop loss or excess loss carrier for the purpose of underwriting, claims adjudication and conducting claim file audits;

(9) Collect protected health information from the individual who is the subject of the protected health information; and

(10) Collect, use or disclose protected health information when the protected health information is obtained from public sources such as newspapers, public agency reports, and law enforcement or public safety reports.

B. Unless otherwise restricted by this section, a carrier that has collected protected health information without an authorization pursuant to Section 11A, may use and

disclose the information to a person acting on behalf of or at the direction of the carrier to perform the insurance functions listed in Section 10H.

C. A carrier shall disclose protected health information in any of the following circumstances:

(1) To federal, state or local governmental authorities to the extent the carrier disclosing the protected health information is required by law to report protected health information or for fraud reporting purposes;

(2) The protected health information is needed for one of the following purposes:

(a) To identify a deceased individual;

(b) To determine the cause and manner of death by a chief medical examiner or the medical examiner's designee; or

(c) To provide necessary protected health information about a deceased individual who is a donor of an anatomical gift;

(3) To a state department of insurance that is performing an examination, investigation, or audit of the carrier; or

(4) Pursuant to a court order issued after the court's determination that the public interest in disclosure outweighs the individual's privacy interest and that the protected health information is not reasonably available by other means.

Drafting Note: States may wish to consider whether they should revise rules of civil procedure to establish appropriate safeguards, including notice mechanisms and protective orders, restricting redisclosure, to protect the rights of individuals who are subjects of protected health information in the context of litigation to which they are nonparties, and to avoid the misuse of subpoenas and discovery requests to circumvent the protections of this Act.

D. A disclosure of protected health information made pursuant to Subsection C shall not be construed to be or to operate as a waiver of privacy rights provided by other federal or state laws, rules of evidence or common law.

Section 12: Disclosure of Protected Health Information Without Authorization for Scientific, Medical and Public Policy Research

A. A carrier may disclose protected health information without authorization to research organizations conducting scientific, medical or public policy research as provided in this Act.

B. (1) A carrier shall keep a record of research organizations to which it discloses protected health information.

(2) The carrier shall keep the record five (5) years.

C. A carrier shall not disclose protected health information to a research organization unless the research organization agrees that the protected health information shall not be disclosed by the research organization to a third person. However, the research organization may disclose the protected health information to its agents, collaborators, or contractors as needed to conduct or assist with the research, as long as all requirements of this section are applied to the agent, collaborator, or contractor.

D. A carrier shall disclose only the minimum data necessary to conduct the intended research. Protected health information shall be disclosed only where identification is necessary to conduct the research.

E. If the scientific, medical or public policy research does not require contact with the individual who is the subject of the protected health information, the following protections shall exist prior to disclosure:

(1) The research organization develops and implements a written policy that includes procedures to assure the security and privacy of protected health information. The policy shall include:

(a) Training and disciplinary procedures to assure that persons involved in research comply with the provisions of this Act;

(b) Safeguards to assure that information in a report of the research project does not contain protected health information. The safeguards shall include a system for ensuring that only authorized individuals are able to establish a link between individuals and their health information; and

(c) A method for removing all information that identifies, directly or indirectly through reference to publicly available information, the individual who is the subject of the protected health information, when the information is no longer needed for research that is

otherwise permitted under this subsection. The policy may also provide that the research organization may retain the protected health information for an indefinite period if archived in an encoded form, and it may not be used for other research unless the requirements of this section are met. "Encoded" as used in this subparagraph means that the personally identifiable information of the data is removed or encrypted and the key to restore the protected health information is retained in a secure place within the research organization with access limited to the minimum number of people necessary to maintain the confidentiality and integrity of the key.

(2) (a) The research organization prepares a research plan that explains the purposes of the research, a general description of research methods to be used, and the potential benefits of the research.

(b) (i) All research plans using protected health information under this Act shall be available to the public and may be obtained by written request to the chief executive officer of the research organization or carrier.

(ii) If the research plan contains information that is proprietary or protected from disclosure by contract or statute, the information may be deleted from the copy made available to the public.

(iii) The research organization shall keep the research plan on file for five (5) years.

(3) (a) The carrier and the research organization shall execute a written agreement:

(i) Stating the purposes of the research;

(ii) Explaining how the purposes qualify as scientific, medical or public policy research;

(iii) Documenting that the organization is qualified under Paragraphs (1) and (2) of this subsection;

(iv) Stating the expected time during which the data will be used for the stated purposes;

(v) Explaining the planned method of disposition of the protected health information at the end of the term of use; and

(vi) Stating that the written agreement shall be available to the public and can be obtained by written request to the chief executive officer of the research organization.

(b) The carrier shall provide a copy of the written, executed agreement upon request to any person. If the executed agreement contains information that is proprietary or protected from disclosure by contract or statute, the information may be deleted from the copy that is made available pursuant to this subsection.

(c) The carrier shall keep this agreement on file five (5) years.

F. If the scientific, medical or public policy research requires contact with the individual who is the subject of protected health information, the following protections shall exist prior to disclosure:

(1) The research organization and carrier shall meet the requirements of Subsection E; and

(2) (a) The research organization is responsible for obtaining a legally effective informed consent of the subject or the subject's legally authorized representative. A research organization shall seek consent only under circumstances that provide the prospective subject or the representative with sufficient opportunity to consider whether to participate in the research, and that minimize the possibility of coercion or undue influence.

(b) The information that is given to the subject or the representative shall be in language understandable to the subject or the representative.

(c) No informed consent, whether oral or written, may include any exculpatory language through which the subject or the representative waives or appears to waive any of the subject's legal rights, or releases or appears to release the investigator, the sponsor, the research organization or its agents from liability or negligence.

(d) Basic elements of informed consent. In seeking informed consent the following information shall be provided to each subject:

(i) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures that are experimental;

(ii) A description of any reasonably foreseeable risks or discomforts to the subject;

(iii) A description of any benefits to the subject or to others that may reasonably be expected from the research;

(iv) A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;

(v) A statement describing the extent to which confidentiality of records identifying the subject will be maintained;

(vi) For research involving more than minimal risk, an explanation as to whether any compensation and medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;

(vii) An explanation of whom to contact for answers to pertinent questions about the research and the research subject's rights;

(viii) The name of a person to contact in the event of a research-related injury to the subject; and

(ix) A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.

(e) Additional elements of informed consent. When appropriate, one or more of the following shall also be provided to each subject:

(i) A statement that the particular treatment or procedure may involve risks to the subject (or to the embryo or fetus, if the subject is or may become pregnant) that are currently unforeseeable;

(ii) Anticipated circumstances under which the subject's participation may be terminated by the investigator without regard to the subject's consent;

(iii) Any additional costs to the subject that may result from participation in the research;

(iv) The consequences of a subject's decision to withdraw from the research and procedures for orderly termination of participation by the subject;

(v) A statement that significant new findings developed during the course of the research that may relate to the subject's willingness to continue participation will be provided to the subject; and

(vi) The approximate number of subjects involved in the study.

(f) If a research organization submits research for approval by an institutional review board under the Federal Policy for the Protection of Human Subjects, as originally published in 56 Federal Register 28000 (1991) and as adopted and implemented by a federal department or agency, compliance with that process will be deemed compliance with the provisions of Subsections E(2) and F(2) of this section.

G. (1) If a carrier discloses to an organization conducting scientific, medical or public policy research health information that is not protected health information because all identifying information is encrypted, the carrier and research organization shall execute a written agreement that provides:

(a) That the research organization will not re-release the data accompanied by the encrypted indentifying information to a third person. However, the research organization may disclose protected health information to its agents, collaborators, or contractors as needed to conduct or assist with the research, as long as all requirements of this section are applied to the agent, collaborator, or subcontractor;

(b) That the research organization shall make no efforts to link any health information it received with encrypted indentifying information to any other data that may identify the individual who is the subject of the information; and

(c) That the research organization shall make no efforts to link any encrypted protected health information with any other identifiable data.

(2) Prior to any encrypted information being decrypted or linked to identifying data, the research organization shall comply with the requirements set forth in this section and health information with decrypted identifying information shall be deemed protected health information.

H. Nothing in this Act shall be construed to prevent the creation, use or release of anonymized data for which there is no reasonable basis to believe that the information could be used to identify an individual.

I. Nothing in this section shall be construed as superseding federal laws and regulations governing scientific, medical and public policy research.

Section 13. Unauthorized Collection, Use or Disclosure of Protected Health Information

An unauthorized collection, use or disclosure of protected health information by a carrier is prohibited and subject to the penalties set forth in Section 15. An unauthorized collection, use or disclosure includes:

A. Unauthorized publication of protected health information;

B. Unauthorized collection, use or disclosure of protected health information for personal or professional gain, including unauthorized research that does not meet the requirements of this Act;

C. Unauthorized sale of protected health information;

D. Unauthorized manipulation of coded or encrypted health information that reveals protected health information; and

E. Use of deception, fraud, or threat to procure authorization to collect, use or disclose protected health information.

Section 14. Right to Limit Disclosures

A. A carrier shall limit disclosure of information, including health information, about an individual who is the subject of the information if the individual clearly states in writing that disclosure to specified individuals of all or part of that information could jeopardize the safety of the individual. Disclosure of information under this

subsection shall be limited consistent with the individual's request, such as a request for the carrier to not release any information to a spouse to prevent domestic violence.

B. Except as otherwise required by law, a carrier shall not disclose protected health information concerning health services related to reproductive health, sexually transmitted diseases, substance abuse and behavioral health, including mailing appointment notices, calling the home to confirm appointments, or mailing a bill or explanation of benefits to a policyholder or certificateholder, if the individual who is the subject of the protected health information makes a written request. The written request shall include information as to how any amounts payable by the individual will be handled. In addition, a carrier shall not require the individual to obtain the policyholder's or certificateholder's authorization to receive health care services or to submit a claim. Except as provided in Subsection C, this section shall not apply to minors.

Drafting Note: States are reminded to ensure consistency with existing state laws addressing privacy of information related to specific health services and to amend the list of services in Subsection B accordingly.

C. (1) A carrier shall recognize the right of any minor who may obtain health care without the consent of a parent or legal guardian pursuant to state or federal law, to exclusively exercise rights granted under this Act regarding health information; and

(2) A carrier shall not disclose any protected health information related to any health care service to which the minor has lawfully consented, including mailing appointment notices, calling the home to confirm appointments, or mailing a bill or explanation of benefits to a policyholder or certificateholder, without the express authorization of the minor. In addition, a carrier shall not require the minor to obtain the policyholder's or certificateholder's authorization to receive health care services to submit a claim.

Drafting Note: The age of consent and the health care services to which a minor may consent may vary depending on state law. Health care services to which a minor may consent typically include those relating to reproductive health services, sexually transmitted disease, substance abuse and behavioral health.

Drafting Note: States should examine existing state laws and amend statutes that conflict with this section, such as laws that require the carrier to send explanations of benefits to policyholders.

D. A carrier that cannot comply with the requirements of this section relating to the suppression of benefit, payment and similar information by the effective date of this Act because of demonstrated financial or technological burdens may make a written request to the commissioner for an extension of the time permitted for compliance. The request shall propose a plan and a timetable for compliance not to exceed eighteen (18) months after the effective date of this Act. Carriers that are granted an extension by the commissioner shall report this extension and the lack of current compliance with the provisions of this section in the notice of health information policies, standards and procedures required by Section 6.

Section 15. Sanctions

Drafting Note: Insert the title of the regulatory official charged with prosecuting violations of the law on behalf of the insurance department wherever the term "commissioner" appears in this section.

A. Civil Sanctions

(1) Whenever the commissioner has reason to believe that a person has committed gross negligence in violation of a material provision of this Act and that an action under this section is in the public interest, the commissioner may bring an action to enjoin violations of this Act. An injunction issued under this section shall be issued without bond.

(2) In addition to the relief available pursuant to Paragraph (1) of this subsection, the commissioner may request and the court may order any other temporary or permanent relief as may be in the public interest, including any of the following, or any combination of the following:

(a) A civil penalty of not more than $10,000 for each violation, not to exceed $50,000 in the aggregate for multiple violations;

(b) A civil penalty of not more than $250,000 if the court finds that violations of this Act have occurred with sufficient frequency to constitute a general business practice; and

(c) Reasonable attorney fees, investigation and court costs.

Drafting Note: States should consider, consistent with existing state laws, whether they wish to allow a private right of action to individuals aggrieved by a violation of this Act.

B. Criminal Sanctions

(1) The penalties described in Paragraph (2) of this subsection shall apply to a person that collects, uses or discloses protected health information in knowing violation of this Act.

(2) A person described in Paragraph (1) shall:

(a) Be fined not more than $50,000, imprisoned not more than one year; or both;

(b) If the offense is committed under false pretenses, be fined not more than $250,000, imprisoned not more than five (5) years, or any combination of these penalties; or

(c) If the offense is committed with the intent to sell, transfer or use protected health information for malicious harm, be fined not more than $500,000, imprisoned not more than ten (10) years, or any combination of these penalties.

C. In any claim made under this section relating to an unauthorized disclosure in which a carrier is being sued under a theory of vicarious liability for the actions or omissions of the carrier's employees, it shall be an affirmative defense that the carrier substantially complied with the requirements of Section 5 of this Act.

D. An individual may not maintain an action against a carrier that disclosed protected health information in good faith reliance on the individual's authorization, if that authorization meets the requirements of Section 10 of this Act and if the disclosure was made in compliance with the requirements of this Act.

E. A person may not maintain an action against a carrier for refusing to provide information or limiting disclosure of protected health information when the refusal or limitation is based upon an individual's request pursuant to Section 14 of this Act.

Section 16. Regulations

The commissioner may, after notice and hearing, promulgate regulations to carry out the provisions of this Act. The regulations shall be subject to review in accordance with [insert statutory citation providing for administrative rulemaking and review of regulations].

Section 17. Separability

If any provision of this Act, or the application of the provision to any person or circumstance shall be held invalid, the remainder of the Act, and the application of the provision to persons or circumstances other than those to which it is held invalid, shall not be affected.

Section 18. Effective Date

This Act shall take effect on [insert a date that allows at least a one year interval between the date of enactment and the effective date.]

Legislative History (all references are to the Proceedings of the NAIC).

1998 Proc. 2nd Quarter (adopted).

Testimony of the

American Psychiatric Association

on

H.R. 4585

The Medical Financial Privacy Protection Act

before the

Committee on Banking and Financial Services

U.S. House of Representatives

Presented by Richard K. Harding, M.D.

June 14, 2000

TABLE OF CONTENTS

Mr. Chair, I am Richard Harding, M.D.,Vice-Chairman of Clinical Affairs and Professor of Neuropsychiatry and Pediatrics at the University of South Carolina School of Medicine. In addition to treating patients and my responsibilities at the School of Medicine, I am President-Elect of the American Psychiatric Association and serve on the

National Committee on Vital and Health Statistics – the panel that advises the U.S. Secretary of Health and Human Services on medical privacy and health information issues.

Thank you Chairman Leach, Ranking Member LaFalce, Mrs. Roukema, Mr. Vento and other members of the Committee for this opportunity to testify. The views I am presenting today are both my views and the views of the APA.

We now face what a bipartisan national panel of experts called a "health privacy crisis". Some observers would even say this view represents an understatement; just several months ago a leading computer magazine proclaimed on its cover "We know everything about you...Privacy is dead; get used to it." What's clear is that today, we live with a 21st Century cyberspace financial and health care system, but we live with medical privacy protections designed for the bygone black and white television era of Marcus Welby, MD.

Fortunately, a groundswell of public opposition is developing to the numerous invasions of privacy confronting us. Groups as diverse as Phyllis Schafly's Eagle Forum, the American Medical Association, major patient groups and the ACLU all believe it is critically important to address the dramatic loss of medical privacy. However, in my opinion, those "inside the beltway" are only beginning to realize the great extent of the public's discontent with the loss of their privacy.

Your efforts Mr. Chairman, as well as those of the Clinton Administration, Mr. LaFalce, and Mr. Markey, to add needed privacy protections to the Financial Services Modernization Act are very important first steps to address the public's concern. We strongly urge you and your colleagues to come together on a bipartisan basis and pass legislation to add critically needed privacy protections to the financial modernization law. Mr. Chairman, while we believe there are issues still to be resolved, we welcome your valuable legislation and look forward to working with you to advance medical privacy.

As we consider this issue I hope each of us will think not only in terms of public policy but also in terms of our own medical records and our own family's privacy. Medical records contain some of the most personal information about ourselves and our families. I can assure you as a patient I want to make the choice myself as to whether my medical information is disclosed, and I want members of my family to have that same right. This decision should ***not*** be made for us by a financial institution. This is ***not*** information that a life insurance salesman, a telemarketer, or a bank's mortgage officer should have at their fingertips. Disclosure of certain medical records information can jeopardize our careers, our friendships, our marriages and even our health.

Financial services modernization and medical privacy.

How, you might ask, could a financial modernization law affect your medical privacy? Simply put, as a result of the 1999 financial modernization law, insurers, including health and life insurers, can merge easily with banks and other financial services companies. As a result, in these large new holding companies it is easy for a health insurance company to disclose medical records information to a corporate affiliate such as a life insurance company, mortgage lender or credit card issuer.

As a result of these disclosures customers and patients can be harmed in many ways. The most obvious example is that medical records would be disclosed to an affiliated banking company. The individual would be denied credit on the basis of his or her medical condition. Affiliates and others could also use customer medical information for marketing and other purposes. But there are additional areas of concern as well. For example, will individuals face discrimination and not be able to obtain health insurance or life insurance they need to protect themselves and their families? And of course the original law contains virtually no limits on police access to records maintained by financial institutions.

Privacy is an essential component of effective medical treatment.

In addition to the importance of privacy in our consumer transactions, personal relationships and professional lives, patient privacy is needed for physicians to provide the highest quality medical care. It is too often forgotten that doctor-patient confidentiality is an essential element for effective medical treatment. Without a very high level of patient privacy, many patients will be deterred from seeking needed health care and from making a full and frank disclosure of information needed for their treatment. After all, the information in our medical records can include information on heart disease and high blood pressure, terminal illness, domestic violence and other women's health issues, psychiatric treatment, alcoholism and other sensitive issues. Patients' legitimate fears about medical privacy if unaddressed by policymakers can also compromise the integrity of research data needed for scientists to make breakthroughs in treating illness and disease. Unfortunately, the more people who see our medical records in a financial institution, the more likely our records will be disclosed and the greater chance that patients will be afraid to seek treatment and provide the fullest information possible to their physicians.

In reference to mental health, privacy is essential for effective psychiatric care. As even the U.S. Supreme Court recognized in its 1996 *Jaffee v. Redmond* decision, mental health information is so sensitive that ***additional*** privacy protections are needed for psychiatric treatment. The Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust...disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure... may impede the development of the confidential relationship necessary for successful treatment." The 1999 U.S. Surgeon General's Report on Mental Health reached a similar conclusion, i.e. that patient consent was an essential component of access to effective psychiatric care.

It is often extremely difficult for individuals to bring themselves to seek mental health treatment. Even in cases where the person is extremely emotionally distressed the individual may still avoid medical care at great cost to themselves and their families. Unfortunately, today these individuals also must overcome their fears that their privacy will be compromised if they seek treatment. I do not believe we as a society should create any additional barriers for effective psychiatric treatment.

Provisions of H.R. 4585 and APA recommendations

The introduction of H.R. 4585 has added a key new element to the privacy debate by focusing exclusively on the medical privacy provisions of the Financial Services Modernization Act. A similar positive development has occurred in the Senate where Senator Shelby is attempting to add a medical privacy amendment to legislation before the Senate Banking Committee. When taken together, these efforts offer the hope of progress on adding urgently needed privacy provisions to the Financial Services Modernization Act.

APA believes that H.R. 4585 creates a valuable framework for protecting medical privacy, and we look forward to working with the committee to insure that the specific provisions of the bill insure that consumers benefit fully from the legislation's protections. H.R. 4585 establishes a key principle for protecting the medical records held by financial services companies. The legislation would create a general rule allowing patients to choose if their medical records will be disclosed to an affiliated company or to a non-affiliated third party. In these cases companies would need the express written consent of the patient before disclosing medical records. We strongly support this patient consent rule. This broad rule is clearly preferable to enumerating specific purposes which require patient consent.

I am equally enthusiastic about the bill's general rule insuring that patients' mental health records will not be disclosed without the patient's separate and specific consent. As I outlined earlier in my testimony, providing patients with this additional right is a sound business practice and, as the U.S. Surgeon General, the U.S. Supreme Court, and others have recognized, privacy is an essential component of effective psychiatric treatment.

The provisions of Representative Leach's bill which allow consumers to decide if their information would be included in lists containing health information - lists which may be used to discriminate against them- are also valuable. In addition, the provisions insure that patients would be able to decide if disclosures of information on their spending habits (such as credit card payment information) is disclosed. In some cases this information can reveal the patient's health condition.

However, I would be remiss not to state my belief that the wide scope of the exceptions to the legislation's patient consent provisions needs to be discussed and reevaluated. For example, the legislation seems to recognize that strong protections are needed to insure that patients can elect to keep their medical records private without compromising their ability to obtain credit. After all if a mortgage lender can make consumers consent to release their medical records as a condition of receiving a loan little would be accomplished. Yet, as currently drafted, do these provisions insure that in the routine course of business patient consent will be voluntary and non-coerced? This remains unclear. I would also like to point out that virtually all exceptions from the original Financial Services Modernization Act's privacy provisions are again included verbatim by reference in this legislation and that the Secretary is given new authority to create additional exceptions. Given the uncertainty surrounding the scope of the bill's exceptions, we look forward to working with members of the Committee to ensure that consumers "in the real world" truly enjoy meaningful new protections. We look forward to resolving these questions with members of the Committee.

A Broad Array of Legislation to add urgently needed privacy protection to the

Financial Services Modernization Act

As part of the Committee's deliberation on H.R. 4585, we believe the Committee should also review several other important bills before the Committee. Ranking Member LaFalce, working closely with the Clinton Administration, has introduced a very valuable and far reaching bill to provide needed medical ***and*** financial privacy protections to the Financial Services law. Likewise, Representative Ed Markey was the first to introduce, with Representative Joe Barton, comprehensive legislation to provide stronger medical ***and*** financial privacy protections to the Financial Services Modernization Act. Mr. Markey's legislation is a very privacy protective bill, and Mr. Markey and Mr. Barton as Co-Chairs of the bipartisan House Privacy Caucus have very actively campaigned for urgently needed improvements in the law.

As Congress focuses greater attention on medical records privacy issues the American Psychiatric Association looks forward to building support for valuable patient privacy proposals. Last summer during the Congress' final deliberations on the financial services bill APA led an ad-hoc coalition of over 40 groups, including key physician, provider, and patient groups as well as major unions and conservative family organizations, which all advocated for meaningful medical records privacy provisions. We look forward to working with these groups again in order to build support for needed medical privacy protections. Thank you for inviting me to testify and I look forward to continuing to work with you and members of the Committee on these issues.

Statement of
Steve Bartlett
President
The Financial Services Roundtable
Before the
Committee on Banking and Financial Services
U.S. House of Representatives
on
H.R. 4585, the Medical Financial Privacy Protection Act
June 14, 2000

Good morning, Mr. Chairman and Members of the Committee.

The Financial Services Roundtable appreciates the opportunity to testify on H.R. 4585, the Medical Financial Privacy Protection Act. The Financial Services Roundtable is a national association of 100 of the nation's largest integrated financial services firms. The members of the Roundtable engage in banking, securities, insurance, and other financial services activities.

H.R. 4585 addresses an issue that is of importance to all members of The Financial Services Roundtable and all consumers of financial services — the privacy of health information in the possession of a financial institution. We support the purpose of this legislation. In fact, as I discuss later in this statement, the Roundtable believes that protecting the confidentiality of health information in the possession of a financial institution is a matter that merits a uniform, national policy.

Also, I believe it is important to note at the outset of this statement that the members of the Roundtable – and as far as I know most providers of financial services – do not currently use health information derived from customers other than for medical reasons or as otherwise intended by customers. In other words, this issue is, at best, a potential "loophole" in our privacy laws.

The Roundtable Supports H.R. 4585

As integrated financial services providers, the members of the Roundtable believe that the sharing of consumer information with affiliates and third parties can benefit the consumers of financial services. Information sharing between affiliates, for example, can permit an integrated firm to structure products and services that meet a consumer's specific needs.

At the same time, the Roundtable's members recognize that financial institutions have an obligation to maintain the confidentiality of certain information within their possession. As a result, the Roundtable joined the rest of the financial services industry in supporting the privacy provisions in the Gramm-Leach-Bliley Act. As the members of this Committee know, the House version of the Gramm-Leach-Bliley Act included provisions protecting health information. The Roundtable supported those provisions, but they were dropped for various reasons. I commend the Chairman for his efforts.

H.R. 4585 would expand upon the privacy provisions in the Gramm-Leach-Bliley Act by establishing new standards for the protection of health information held by financial institutions. The Gramm-Leach-Bliley Act provides that a financial institution may not disclose personal information to a non-affiliated third party, without giving the consumer an appropriate notice and opportunity to prevent such disclosure. H.R. 4585 would impose a more stringent standard for health information. It would prevent a financial institution from sharing health information without the affirmative consent of the consumer. Furthermore, the bill's limitations on the sharing of health information would apply not only to non-affiliated third parties, but also to any affiliate of a financial institution.

The Roundtable supports the protections for health information contained in H.R. 4585. The

Roundtable's members recognize that health information can be more sensitive than other forms of personal information. Roundtable members also know that consumers provide medical information to financial institutions only for specific purposes, such as the purchase of insurance, and the Roundtable members limit the use of such information accordingly.

Financial Institutions Already Protect Health Information

Our support for H.R. 4585 is a reflection of current industry practice. Almost every state has adopted some law to protect the confidentiality of health information, and, in most states, health information cannot be disclosed without the affirmative consent of an individual.

Additionally, the financial services industry has voluntarily agreed to safeguard health information within its possession. Just last month, for example, the Roundtable joined the nation's major banking trade associations in the release of voluntary guidelines for the banking industry which call for a banking institution to obtain the affirmative consent of a customer before sharing health information. It is my understanding that the major national insurance trade groups have adopted similar policies for insurance companies.

The U.S. Department of Health and Human Services (HHS) also is in the midst of finalizing regulations that relate to the privacy of health information.

As the Committee continues its deliberations of H.R. 4585, we would urge it to review and take into account this framework of existing law and industry guidelines.

Certain Provisions in H.R. 4585 Need to be Revised

Our support for H.R. 4585 is not unqualified. While we believe that the sharing of health information should be subject to a policy of affirmative consent, we also believe that the bill should be revised in several respects. The following are some of our concerns.

Exceptions to the Affirmative Consent Requirement

Under H.R. 4585, most of the exceptions to the sharing of personal information that are contained in the Gramm-Leach-Bliley Act would apply to the sharing of health information. For example, the bill would permit a financial institution to share health information with another party to protect against or prevent actual or potential fraud or claims. However, the bill does not extend two of the exceptions in the Gramm-Leach-Bliley Act to health information, and these two exceptions should apply to the sharing of health information.

First, the bill would not allow an insurance firm to share information with an insurance rate advisory organization or a state insurance guaranty fund without affirmative consent. Insurance companies share health information with rate advisory organizations to establish rates for particular lines of insurance. Similarly, when an insurer is declared insolvent, health information in its possession must be shared with a state guaranty fund. If such information cannot be shared freely with rating organizations or guaranty funds, the establishment of rates and resolution of insolvencies may be seriously impaired. We urge the Committee to include the Gramm-Leach-Bliley exception for information sharing with rate advisory organizations and state guaranty funds.

The absence of this exception is a serious flaw in the current draft; one which I hope is inadvertent. Without this exception, the basis for pricing insurance products and resolving insolvencies of insurance firms could be seriously harmed. I do not believe that is the intent of Congress or the will of the American people.

Second, the Gramm-Leach-Bliley Act includes an exception for the sharing of information with service providers and joint marketers as long as such parties maintain the confidentiality of the information. We believe a similar exception should be included in H.R. 4585. Without such an exception, it would be difficult for many insurance firms to use independent agents, banks, broker/dealers or others to service

or market products, and this could have a negative impact on the consumers of insurance products.

Additionally, the Committee should consider exceptions for other current industry practices. For example, the operation of worker's compensation programs and medical research programs depends heavily on the sharing of information between insurance companies and third parties. The effectiveness of these programs could be impaired by the application of the affirmative consent requirement.

Consumer Rights to Access and Corrections

H.R. 4585 would provide consumers with a right to review health information in the possession of a financial institution and a right to dispute the accuracy of such information. While we endorse the intent of these provisions, we believe that they deserve further consideration by the Committee.

First, the Committee should recognize that there are instances in which it is not appropriate for a financial institution to share unconditionally health information with a consumer. Consider, for example, a situation in which a life insurance company learns through a required blood test that an applicant for life insurance is HIV positive. Because of the sensitive nature of this information, most insurance companies currently will not convey the results of such a test directly to the applicant, but will notify the applicant's doctor and rely on the applicant's doctor or a trained counselor to convey that information. Some states have addressed this and similar situations by limiting an individual's access to health information that could endanger the life or safety of the individual.

Second, the Committee should clarify that a financial institution has an obligation to "amend, correct, or delete" health information that is incomplete or inaccurate only if the financial institution created such information. As drafted, H.R. 4585 implies that a financial institution has some obligation to amend, correct, or delete any incomplete or inaccurate information, regardless of who created the information.

Third, H.R. 4585 would provide that a consumer does not have a right to obtain information assembled by a financial institution as part of its efforts to "comply" with laws preventing fraud. We recommend that this exception also include information assembled to "identify or investigate" possible fraud, as well as information assembled in the context of a dispute with the consumer.

Finally, the Committee should consider what procedures apply to these provisions. For example, does the consumer's right apply to all information, no matter when created? How quickly must a financial institution respond to a request for information? If there is a dispute over the accuracy of the information, how is that dispute to be adjudicated?

Spending Habits and Aggregate Lists

The affirmative consent requirement in H.R. 4585 would apply to the compilation of lists and descriptions of consumer spending habits if such lists and descriptions are derived from health information. Also, the affirmative consent requirement would apply to the compilation of aggregate lists of consumers that contain or are derived from health information. Presumably, these provisions are intended to limit the use of health information for marketing purposes. However, as drafted, the provisions would limit the sharing of experience information between an insurance company and third parties, including affiliates that use such information to develop generic claims profiles and insurance rates. Also, care needs to be taken to ensure that these provisions do not affect aggregated lists of credit card charges and checking account activities currently provided to consumers. To avoid such problems, we recommend that these provisions be limited to "marketing" activities.

Treatment of Mental Health Information

H.R. 4585 would require a financial institution to obtain a separate consent from a consumer before sharing any information related to the mental health or mental condition of the consumer. This means that in certain cases a financial institution would be required to obtain two, separate consents from a consumer — one governing the consumer's "individually identifiable health information," and a second specifically related to the consumer's "mental health or mental condition." We do not see the need for

this double consent requirement. The bill's definition of "individually identifiable health information" expressly includes any information related to the "physical or mental health or condition" of an consumer. One consent should be sufficient.

Additionally, the bill does not define what constitutes "mental health" or "mental condition." If any provisions specifically relating to these terms are included in the bill, we urge the Committee to define them.

Definition of "Individually Identifiable Health Information"

We are concerned about the relationship between the protections for health information in H.R. 4585 and the protections for personal information that already are part of the Gramm-Leach-Bliley Act. The existing privacy provisions in the Gramm-Leach-Bliley Act do not prohibit the sharing of demographic information about a consumer, such as an individual's address, telephone number or zip code, if that information is publicly available. On the other hand, H.R. 4585 would prohibit the sharing of demographic information created by an employer or health care entity that relates to an individual's health and that identifies the individual. In order to avoid any confusion with the Gramm-Leach-Bliley Act, we believe the Committee should clarify that publicly available demographic information that does not include health information is not subject to the affirmative consent requirement imposed by the bill.

The Need for a National Standard

As I noted at the outset of this statement, the Roundtable believes that the confidentiality of health information is a matter that merits a national policy approach. In other words, it is a concern to all consumers and all financial institutions that possess health information. As a result, the Roundtable believes that maintaining the confidentiality of health information demands a uniform, national policy.

All consumers, regardless of where they reside or receive health care, should be able to expect the same level of protection for their health information. Similarly, all financial institutions that possess health information should be able to comply with one national set of confidentiality requirements.

Absent a single, national standard governing the confidentiality of health information held by financial institutions, the customers of those institutions and the institutions themselves will face a patchwork of requirements imposed by state and federal legislators and regulators. As I have previously noted, most states already have adopted laws governing the confidentiality of health information, and HHS is in the process of finalizing a regulation on this issue. These requirements, however, are far from uniform or comprehensive.

The Committee faces an important choice. It can either layer the requirements of H.R. 4585 on this existing patchwork of laws and regulations and thereby add to the confusion of consumers and the compliance burden of financial institutions, or it can establish a single national standard governing the confidentiality of health information maintained by financial institutions. The Roundtable would recommend that the Committee impose a national standard. Thank you for the opportunity to share our views on this important and timely topic.

DONALD C. BRAIN, JR., CPA, AAI
PRESIDENT
LOCKTON BENEFIT GROUP
ON BEHALF OF THE

INDEPENDENT INSURANCE AGENTS OF AMERICA
NATIONAL ASSOCIATION OF INSURANCE AND FINANCIAL ADVISORS
NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

BEFORE THE HOUSE COMMITTEE ON BANKING
AND FINANCIAL SERVICES

JUNE 14, 2000

Mr. Chairman, and members of the Committee, my name is Don Brain. I am the President of the Lockton Benefit Group, the 11th largest benefits consulting firm in the nation. The 3,000-employee Lockton Benefit Group sells and administrates a full range of employee benefit plans. I appear today on behalf of the insurance agents and brokers of America, and their employees – nearly 1,000,000 men and women who work in every part of the United States. These professionals are represented by the Independent Insurance Agents of America, Inc. (IIAA), the National Association of Insurance and Financial Advisors (NAIFA, formerly known as NALU) and the National Association of Professional Insurance Agents (PIA), on whose behalf I testify today.

I currently serve as a member of IIAA's Government Affairs Committee and I am the Health Care Liason to that committee. In addition, many of the Lockton Benefit Group's agent and broker-employees are members of NAIFA and the Association of Health Insurance Advisors, NAIFA's conference devoted exclusively to health insurance and benefits-related issues. IIAA, NAIFA and PIA members include health insurance specialists located across the country, and IIAA, NAIFA and PIA represents their members' interests on a wide-range of insurance matters, including health and employee benefits issues.

INTRODUCTION

IIAA, NAIFA and PIA are appearing before you today to comment on the bill that you just recently introduced – H.R. 4585, the "Medical Financial Privacy Act." First, Mr. Chairman, let me thank you for holding this hearing today and providing us with a chance to submit our views on this very important piece of legislation. There is perhaps no more important topic in politics today than ensuring that the private information of individuals remains just that – private. And there is no more important type of information that should remain private than each and every person's medical information.

At the outset, I must therefore commend you, Mr. Chairman, for following up your work on the Gramm-Leach-Bliley Act with legislation designed to strengthen that Act's consumer privacy protections in the health information context. I also must commend you, Mr. Chairman, for being sensitive to our views and for agreeing to work with us to ensure that the protections that you are crafting protect consumers' privacy while at the same time protecting their access to employer-sponsored group health care plans.

The primary message that I have been asked to relate to you today, Mr. Chairman, is that the insurance agents want you to know that they intend to do everything within their power to help you mold a bill that can take flight and become the law of the land.

The insurance agents fully support the overarching objective of protecting individuals' sensitive health information and your approach to achieving that objective. At the same time, insurance agents need to share information that they receive in the normal course of business with insurers and health care providers in order to provide both the high level of service and the health care benefits that all of us want and need. Insurance

agents use the information for one purpose and one purpose alone: to help provide the highest level of health care benefits and service within the budgetary constraints of each of their clients. Indeed, because the vast majority of small businesses in the United States cannot afford a separate health benefits administrator or human resources department, the agent often fills those roles for such small businesses.

From our perspective, the only clarification that is necessary to ensure that the on-going administration of employer-sponsored health benefit plans and workers compensation programs is not disrupted in any way is to specifically provide that information obtained in conjunction with the administration of a plan can be used for any purpose related to the administration or replacement of that plan.

This testimony is divided into two parts. The role of the insurance agent and the manner in which employer-sponsored group health insurance plans and workers compensation programs are administrated is outlined in the first part. The second part then highlights the need for our suggested clarification.

1. The Role and Value of the Agent/Broker

Historically, the agent system has been the principal method of distribution for private life and health insurance. Agents are the essential link between the consumer and the insurance company, providing and servicing the products of the insurer while educating the consumer on how to manage risks and how to make informed choices regarding their insurance purchases.

Dramatic increases in health care costs in the last decade have made the agent an increasingly important part of the health care equation. More than ever, both employers and individuals rely on the advice of their agents regarding cost savings measures and coverage options. Indeed, in the health insurance context, the agent almost always represents the interests of the insured or of the employer-sponsor of the health care plan. In this sense, the agents are acting as "brokers" and they are not considered to be agents of the underwriters.

Health insurance agents/brokers play a number of invaluable roles:

- They work with clients to evaluate their need for health insurance protection. This may involve substantial research and fact finding about the client's needs. It also may involve sharing health information about an employer's employees with a number of different insurers to fully evaluate the potential health benefit plan options and the costs of each of those options.

- They educate by explaining the various health plans available and provide appropriate cost indexes.

- They make specific recommendations that suit the client's objectives and budget. Often a health insurance plan is designed by the agent to fit a client's special needs.

- They encourage the client to act in a timely fashion to assure that the proper coverages are in place when they are needed. They also see to it that accurate and complete information is provided to the insurer to make sure that the client gets the very lowest premium available.

- They keep in touch with the client and review or update coverage on a periodic basis. They suggest changes when appropriate and counsel clients on ways to reduce cost. Often they must assist their client in reviewing the need for legal and tax compliance, recommending other professional assistance when necessary.

- They assist with claims, answer questions and serve as ombudsmen in helping their clients and their clients' employee-insureds deal with insurance companies. Agents often spend a great deal of time helping to assemble the proper documentation needed to file or follow up on a claim.

- They assist business owners in communicating their benefit packages to their employees, often assisting the employee in seeing how the benefits coordinate with their personal financial programs as well as those provided by government entities.

2. The H.R. 4585 Proposal – Protecting The Viability Of Employer-Sponsored Health Benefits

As noted at the outset, IIAA, NAIFA and PIA share the overarching objective of ensuring that the confidentiality of individually identifiable health information is protected. Indeed, IIAA, NAIFA and PIA have fully supported efforts in the States to enact privacy provisions that apply to both insurers and agents. Although H.R. 4585 would help to ensure that these confidentiality objectives are met, it must be clarified to make clear that its restrictions are not intended to interfere with the provision of employer-sponsored group health plans or workers compensation programs in any way.

A failure to make such a clarification could have serious negative ramifications for our current health benefits system. This is because tens of millions Americans currently are insured through employer-sponsored health benefits plans and are protected by state-mandated employer-purchased workers compensation programs. In order to evaluate alternative and replacement benefits plans, agents must be able to use and share personally identifiable health. Indeed, insurers cannot and will not price a group plan without specific information on the claims history of members of that plan. If a single employee directs that their information not be shared for that purpose, the entire group plan would be frozen in place.

Without the clarification we have requested, the legislation would thus undoubtedly serve both to increase the costs of providing health care benefits and to reduce the number of benefit options that many employers will be able to consider. This would greatly undermine the level of care that many Americans will be able to receive and it would likely lead to a tremendous expansion in the number of un- or under-insured Americans.

CONCLUSION

In closing, I would just like to thank you once again for offering us this opportunity to testify. IIAA, NAIFA and PIA look forward to working closely with you to in your efforts to pass H.R. 4585 into law this term. I would be happy to answer any questions.

STATEMENT OF THE AMERICAN INSURANCE ASSOCIATION

Hearing on H.R. 4585, the Medical Financial Privacy Protection Act

Submitted To The
Committee on Banking and Financial Services
United States House of Representatives

June 14, 2000

American Insurance Association
1130 Connecticut Avenue, NW
Suite 1000
Washington, DC 20036
(202) 828-7100

American Insurance Association

The American Insurance Association is a national trade organization of property and casualty insurers.

Testimony of the American Insurance Association before the Committee on Banking and Financial Services, U.S. House of Representatives on H.R. 4585, the Medical Financial Privacy Protection Act

Mr. Chairman and Members of the Committee:

My name is Robert H. Rheel, senior vice president at the Fireman's Fund Insurance Company. I am pleased to appear before you today on behalf of the American Insurance Association to discuss H.R. 4585, the Medical Financial Privacy Protection Act, and we appreciate the opportunity to present our views.

The AIA is the principal trade association for property and casualty insurance companies, representing more than 370 major insurance companies which provide all lines of property and casualty insurance and write more than $60 billion in annual premiums. Fireman's Fund, established in 1863 in San Francisco, California, is among the nation's top writers of property casualty insurance and employs over 8,000 people.

INTRODUCTION

The issue of maintaining the privacy of medical information is a vitally important issue for consumers and for our member companies. As we have stated on several occasions before this Committee and elsewhere, information is the lifeblood of the insurance industry. Without access to customer information, we could not offer and provide insurance products to consumers. We could not process claims, and we could not protect against fraudulent activities. At the same time, we recognize how concerned policyholders are that we preserve the confidentiality of the sensitive medical and financial information we maintain.

Insurance companies have long had experience with maintaining and protecting financial and medical information we collect and possess about our policyholders. Many states have already enacted laws that provide protection for medical and financial information maintained by insurance companies. These laws provide a well-balanced approach to consumer privacy, and provides significant protection at the state level for consumers' medical and financial information while not unduly interfering with the necessary disclosure of information needed to underwrite insurance and process transactions and claims.

The recently enacted, and soon to be effective, privacy provisions of the Gramm-Leach-Bliley Act and rules recently adopted by the federal financial institution regulatory agencies already provide coverage for medical information maintained by financial institutions. We understand that the state insurance

commissioners are considering rules to implement Title V. In view of the importance access to medical information plays in the insurance industry, we have urged the commissioners at this time to defer action on the issue of medical information.

In view of all of these evolving events, we do not believe it is appropriate nor necessary for Congress to adopt legislation at this time. Insurers and other financial institutions are in the process of implementing the Gramm-Leach-Bliley Act and the rules adopted by the agencies and the state insurance regulators. At this time, we do not believe the benefits which the bill purports to provide outweigh the considerable burdens it would clearly impose. We are unaware of any instance of abuses in the property/casualty insurance industry . Further, there are some serious drafting oversights which we believe need be addressed. Finally, adoption of the legislation at this time would prove particularly disruptive, and we believe it to be inappropriate at this time.

THE EXPERIENCE OF THE INSURANCE INDUSTRY WITH PROTECTING MEDICAL INFORMATION IS EXCELLENT

The insurance industry has long recognized that information concerning customers must be protected and not disclosed to third parties except as necessary to facilitate transactions with customers. Insurance companies employ strict procedures to ensure that customer information is used only to carry out our responsibilities under the policies we have entered into with our customers.

Insurance companies have a legitimate need for information about policyholders and claimants. In the context of processing claims, a company finds it necessary to obtain information regarding a claimant in order to decide whether or not to pay a claim. It may be necessary to request claimants to provide medical information as part of the claims processing process. Such information is carefully guarded by insurance companies, and is released to third parties only as necessary to facilitate the processing of the claim.

As the Committee is aware, last November Congress enacted comprehensive legislation that ensures the confidentiality of consumers' personal information maintained by financial institutions, including insurance companies. The legislation requires all financial institutions to provide their privacy policies to customers at the time the customer relationship is established and each year. Financial institutions are not permitted to share personal information about a consumer with a nonaffiliated third party unless the consumer has been notified about the possibility of such disclosures and has not informed the financial institution to keep the information confidential. The rules adopted by the federal agencies provide that medical information maintained by financial institutions is covered by the privacy protections of Title V of the Gramm-Leach-Bliley Act. The rules also provide that the Act goes into effect beginning this November, and that financial institutions are required to comply with all aspects of the rules and legislation by July 1st of next year.

The nation's federally regulated financial institutions are just beginning to implement the rules the agencies adopted last month. In view of the uniqueness of insurance companies, Title V provided that the state insurance commissioners should enforce the privacy provisions applicable to insurance companies. The commissioners, under the auspices of the National Association of Insurance Commissioners, are now in the process of evaluating these rules and proposing privacy rules that would apply to insurance companies. It will undoubtedly be another few months before these rules are adopted. In this regard, the commissioners recently adopted a resolution indicating that they intend to promulgate rules that provide a uniform compliance date of July 1, 2000, which is the same date adopted by the federal regulators.

In addition, the federal agencies and state insurance commissioners are required to develop standards for financial institutions relating to administrative, technical and physical safeguards to insure the security and confidentiality of customer records and information. We believe the insurance industry already has in place effective procedures for protecting the confidentiality and security of our policyholders' personal information, and we are confident that we will meet the standards the agencies adopt.

It is important to recognize that the implementation of Title V is enormously complex. It involves more than just mailing privacy statements to customers. Financial institutions must determine the categories of information they collect and disclose and the categories of third parties to whom they disclose information. Information systems must be modified to maintain the names and other identifying information of customers who do not want their information shared with unaffiliated third parties. These systems must be integrated with existing systems to ensure that the customer's instructions are followed. Financial institutions have advised that it will take at least six months to develop, implement and test the system changes that they have begun to develop. To impose the additional requirements that are called for in H.R. 4585 would result in considerable, unwarranted burdens on financial institutions that are dedicating significant resources to implementing Title V.

THE REQUIREMENTS OF H.R. 4585 ARE NOT NEEDED AT THIS TIME

Opt In Requirements are Inappropriate

The proposed legislation requires financial institutions to obtain the consent of consumers before disclosing any individually identifiable health information. As a practical matter, insurance companies obtain the consent of prospective policyholders to obtain and release health information in connection with processing insurance applications. Nevertheless, we do not believe that the requirement for obtaining the consumer's consent fits well with the requirement of Title V that the consumer be given an opportunity to opt out from proposed disclosures to third parties.

The opt in requirement will be unnecessarily confusing for financial institutions and consumers. The AIA believes that the current opt out provisions of Title V, taken in conjunction with those of the Fair Credit Reporting Act, provide considerable protections for consumers to assure that the confidentiality of their health information will be maintained. Consumers who are concerned with the disclosure of such information will be given numerous opportunities to instruct the financial institutions they do business with not to disclose nonpublic personal information, including health information, with third parties. The agencies' rules provide that notices must be clear and conspicuous, and must give the consumer a reasonable means of opting out. Recognizing, however, that there is a higher level of concern with the sharing of medical information, we are willing to consider a narrowly drafted requirement relating to the sharing of medical information for marketing purposes. We are in the process of discussing such an approach with the National Association of Insurance Commissioners. Such a provision cannot impinge upon an insurer's ability to conduct its core insurance functions. In addition, new requirements should not be imposed until insurers and other financial institutions have had the opportunity to make the systems changes needed to comply with the original provisions of Title V.

Affiliates Should Not be Subject to the Requirements

The Gramm-Leach-Bliley Act provides that financial institutions must disclose to consumers their policies regarding the sharing of information with affiliated and unaffiliated third parties. However, the opt out requirements of Title V apply only to the sharing of information with unaffiliated third parties. The Gramm-Leach-Bliley Act does not cover sharing information with affiliates for several reasons. First, in many instances an affiliate is nothing more than a department of the company. Financial institutions may establish separate subsidiaries for reasons related to licensing, tax and organizational objectives. For example, in view of the state-oriented regulatory structure applicable to the insurance industry, it is commonplace for companies to establish subsidiaries in different states. Information relating to policyholders, however, is often made available among affiliates in order to better serve customers. As a result, the sharing of information among affiliates is tantamount to the company using the information itself for its own business-related purposes. No purpose is served by imposing additional hurdles to the sharing of such information. Indeed, additional burdens on information sharing would undoubtedly reduce the ability of insurance companies to serve its policyholders.

In addition, Title V recognizes that institutions that share information with affiliates already are subject to the Fair Credit Reporting Act. The FCRA provides that an institution may not disclose personal information of its customers (other than transaction and experience information) to an affiliate unless the consumer has been given an opportunity to opt out. As a result, under current law financial institutions may not routinely share health information with affiliates unless they have given consumers an opportunity to opt out from such disclosure.

In view of the carefully crafted language of the Gramm-Leach-Bliley Act, as well as the coverage for affiliate sharing contained in the FCRA, we believe that any further restrictions on the ability of financial institutions to share information with affiliates should await a comprehensive review of the FCRA. In any event, they should not prevent insurance subsidiaries within a holding company structure from sharing medical information that is needed to serve customers.

Restrictions on Information About Personal Spending Habits Are Unnecessary

H.R. 4585 limits the ability of financial institutions to use information relating to payments the consumer has made without the consent of the consumer if such information is derived from individually identifiable health information. While the insurance industry does not ordinarily make use of such information in this manner, we believe that the proposal would have unintended effects.

It is operationally difficult for financial institutions to distinguish between payments that relate to health claims and other payments. Accordingly, the profiling provision of the legislation would apply to all payment information which financial institutions maintain. In view of the broad coverage of this section, this restriction could prove very disruptive to the ongoing operations of financial institutions. Because financial institutions may be unable to separate financial and medical, insurers may not be able to obtain necessary information about a payment which a policyholder may have made without running afoul of this section.

We do not believe that the limited benefits which the provision provides outweighs the considerable operational burdens.

There Is No Reason Why The Exceptions of H.R. 4585 Should Be More Limited Than Those In Title V

In order to avoid serious disruptions to normal operations, Congress wisely adopted several exceptions that permit financial institutions to routinely share customer information with third parties. These include sharing information as necessary to effect, administer or enforce transactions requested or authorized by consumers. Similarly, H.R. 4585 provides a number of exceptions as well to the requirement that the consumer's consent be obtained before health information may be shared.

However, the bill leaves out several exceptions that are important for the insurance industry. For example, Title V permits insurance companies to provide information to insurance rate advisory organizations, state guaranty funds or agencies, rating agencies and persons assessing the financial institution's compliance with industry standards. These exceptions are critical to the insurance industry. We believe the reasons for the exceptions provided in Title V apply with equal force to the sharing of information under H.R. 4585. Accordingly, we urge the Committee to restore the exceptions as provided in Title V.

State guaranty funds and agencies play an important role in connection with the insolvency of insurance companies. These organizations play a role similar to that of the Federal Deposit Insurance Corporation with regard to depository institutions. In the event an insurance company fails, guaranty funds and agencies provide the necessary continuity by stepping in to satisfy claims (including those that relate to payments to cover medical care) of the failed company. In order for them to perform their function effectively, it is imperative that they have access to all information in the insolvent insurance company's files.

Insurance rate advisory organizations, rating agencies and persons assessing the financial institution's compliance with industry standards must have access to a full range of information from insurance companies in order to assesses risk and perform their important evaluative roles. We think it is important for these exemptions to apply to the sharing of health information as well.

Title V also permits a financial institution to disclose information to a third party who is assisting the institution in marketing its products and services if the institution fully discloses this to the customer and the third party contractually agrees to maintain the confidentiality of the information. Because it is quite common for insurance companies to rely upon third parties such as independent agents to market insurance products, it is very important that this exception also apply to the sharing of health information. Without this exception, insurance companies would be unable to continue to use their current marketing channels.

Another exception provided for in Title V which was not carried through to H.R. 4585 is the provision which permits financial institutions to provide information to consumer reporting agencies in accordance with the Fair Credit reporting Act or from a consumer report by a consumer reporting agency. We believe that this is an important exception, particularly in view of the broad scope of the definition of the term "individually identifiable health information." As the Committee is aware, the FCRA imposes severe limitations on the ability of consumer reporting agencies to provide information to requestors. It is important for the smooth functioning of the insurance industry that companies be able to provide information to consumer reporting agencies and that we be able to make use of information provided by such agencies.

RESTRAINTS ON INFORMATION REQUESTS

We are puzzled by the requirement contained in H.R. 4584 that in connection with considering a loan request, financial institutions may not use information from an affiliate unless they normally receive the same information from unaffiliated parties. If a financial institution believes it is desirable to obtain information from an affiliate, we see no public policy reason why the consumer should not be able provide his or her consent to permit the affiliate to share the information with the financial institution. It is cumbersome and inefficient to require the financial institution to seek

information from other sources, and we cannot understand what purpose is served by such a requirement.

ACCESS AND CORRECTION RIGHTS

H.R. 4585 requires financial institutions to make available to consumers individually identifiable health information which the institution possesses, and provide the consumer with an opportunity to request that inaccurate information be corrected. The AIA believes that such access should be limited only in instances where the consumer's application is denied based upon the health information contained in the institution's records. We see little purpose to be served in providing access to such information when the consumer has not been denied a product or service by the financial institution. The burden and expense that financial institutions would incur in order to provide access to such information to consumers who were not denied products and services far outweighs the benefits.

We also believe it important that customers not be given access to certain confidential information, such as information insurance companies maintain in connection with investigating fraud, misrepresentation, unlawful activity, and information developed in connection with litigation. Permitting customers to obtain access to such information would have an adverse effect upon the ability of financial institutions to investigate illegal activity and defend themselves against improper activities.

CONCLUSION

In summary, we want to underscore that insurers understand and appreciate that consumer privacy, especially as it relates to financial and medical information, is a top public policy concern. We believe the experience of the property / casualty insurance industry demonstrates that confidential health information is presently being protected by companies and we know that we must remain ever vigilant to protect this information in order to maintain our policyholders' confidence. However, in our effort to secure this information, legitimate disclosures of information needed to continue to provide our customers with the insurance protection they require should not be restricted. We look forward to working with the Chairman and Members of the Committee on this very important issue.

Testimony of

Edward L. Yingling

On Behalf of the

American Bankers Association

Before the

Committee on Banking and Financial Services

United States House of Representatives

June 14, 2000

Testimony of Edward L. Yingling
On Behalf of the American Bankers Association
Before the
Committee on Banking and Financial Services
United States House of Representatives
June 14, 2000

Mr. Chairman, I am Edward Yingling, Deputy Executive Vice President and Executive Director of Government Relations for the American Bankers Association (ABA). ABA brings together all elements of the banking community to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional, and money center banks and holding companies, as well as savings institutions, trust companies, and savings banks – makes ABA the largest banking trade association in the country.

Mr. Chairman, thank you for holding this hearing on medical privacy. The issue of privacy – that is, the responsible use and protection of customer information – is the ABA's top priority. The banking industry has a long history of earning the trust of its customers and, in particular, of protecting their private financial information. Indeed, our extensive survey work shows that consumers trust banks more than virtually any other institution to protect their information.

We are now in the middle of a revolution in information technology. This rapidly changing technology landscape raises exciting new possibilities to provide customers with new and innovative products, to increase convenience, and to lower costs. At the same time, this changing technology raises important questions about the appropriate use of information and the need to make sure we meet the expectations of our customers that information be used responsibly. While technologies have changed, the fundamental principle of protecting customer information and preserving trust has not – it remains the cornerstone of successful banking.

It would seem obvious that medical information is at the top of the list of information about which consumers are concerned, and, indeed, our survey work confirms that. Throughout its history, the banking industry has protected the medical information of its customers whenever

that information has been made available to banks. Therefore, our industry's basic approach to medical information is straightforward: ***Medical information should only be used for the express purpose for which it is provided and should not be shared without the express consent of the customer***. More specifically, concern has been expressed that lenders might use medical information obtained elsewhere in making a credit decision. ABA's position is that such use of medical information in a credit decision obtained without the knowledge and consent of the borrower is just plain wrong. There are instances where medical information is relevant – for example, in sole proprietorships or small businesses where the franchise value of the firm hinges on one or two key individuals. In such cases, insurance on the key individuals might be required. However, in those instances, the prospective borrower will know what information is required, and can expressly consent to its being obtained and used. Otherwise medical information should not be used.

On June 6, the ABA, joined by the Financial Services Roundtable and the Consumer Bankers Association, announced new voluntary guidelines on the appropriate use and protection of information, based on the extensive work of a blue ribbon ABA task force. Attached to this testimony is a copy of those guidelines. The guidelines represent core values for our industry. The guidelines will help bankers reassess every aspect of how they collect, use and distribute information – from who sees the information, to how it is stored and updated; from how it is used to benefit the customer, to how it is protected.

We believe one of the most important guidelines is number 3, which states:

Medical Information Will Not Be Shared

Financial institutions recognize that, when consumers provide medical information for a specific purpose, they do not wish it to be used for other purposes, such as for marketing, or in making a credit decision. If a customer provides personal medical information to a financial institution, the financial institution will not disclose the information, unless authorized by the customer.

In addition, last year the ABA supported the legislative provisions on medical privacy that were contained in early versions of what became the Gramm-Leach-Bliley Act. We were disappointed that the issue was not addressed in that legislation last year.

Therefore, ABA can clearly support the thrust behind H.R. 4585. Having said this, I must also say that the ABA has very serious concerns relating to H.R. 4585 in two areas. The first relates to process. While it may indeed be possible to obtain a broad consensus on a targeted bill on medical information, I want to emphasize that the ABA, and I believe the financial services industry generally, would be strongly opposed to opening up the privacy provisions of Gramm-Leach-Bliley on a broader front. Given the limited number of legislative days left in this Congress, any attempt to broaden the legislation would likely mean that there would be no legislation at all.

It should be clear to everyone by this time that privacy is a tremendously complex area – and one where the law of unintended consequences is very much in play. We recognize that some members of this Committee did not feel that the privacy provisions in Gramm-Leach-Bliley went far enough, but one has only to look at the length and complexity of the regulations just finalized to realize what a major piece of legislation the privacy provisions were. The ABA strongly believes that we need to see just how the current law works before we try to add additional requirements to it.

A special word is in order about regulatory costs. Our members are now beginning to estimate the cost of compliance with the new privacy law, and it is clear for the largest banking institutions that it will be in the tens of millions of dollars each. Indeed, we believe it is a conservative estimate that the initial cost across all financial services firms will be in excess of $1 billion, with additional ongoing costs each year. These costs include developing the privacy programs, reworking all information systems throughout each institution to comply with those programs, training virtually every employee within an institution, and developing and mailing the privacy notices. It is, of course, the case that in a competitive market – like that for financial services – it is the consumers of the products and services that ultimately pay most of these costs.

A second area of concern relates to some of the specific provisions in H.R. 4585. Working with our colleagues in the Financial Services Coordinating Council (FSCC), we have identified a number of specific problems in the bill that need to be addressed. (The FSCC consists of the ABA, the American Insurance Association, the American Council of Life Insurers, the Investment Company Institute, and the Securities Industry Association.) In particular, there are specific recommendations from the insurance industry relating to long-standing underwriting processes that are used to develop appropriate insurance models. ABA urges the Committee to listen carefully to those concerns and to address them in any mark-up of this bill.

Furthermore, the ABA has a very real concern with the subsection in the bill relating to "Consumer Rights to Access and Correct Information." Simply put, we find this provision totally unworkable in the real world. The concept of having a consumer be able to see his or her medical information and to correct it is likely based on the Fair Credit Reporting Act (FCRA). Under that act, consumers are given the right to see their information in their individual credit file and to ask that any misinformation be corrected. There are two very important differences between the FCRA and the consumer access provision in H.R. 4585. First, under FCRA, the request to see information relates to a very specific credit file. The entire function of credit bureaus is to develop a report on individuals, and, therefore, information is centralized into that one file. In fact, the purpose of credit bureaus is to collect ***in one place*** credit information from many sources so that a lending institution relying on a credit report will have the full history of the perspective borrower. On the other hand, banks generally do not collect medical information on customers. Whatever information a bank may have access to is a natural consequence of providing services, such as payment system services (e.g., checking, credit card, and debit card services). Because such information is not collected and stored in one place such as a specific file, it would be difficult if not impossible for a bank to retrieve with confidence any medical information that it may have access to. In fact, we would think Congress would not want us to collect it in a central location.

Secondly, the FCRA is designed to protect the information that is used for a very important purpose – making credit decisions. Credit bureaus deliberately collect this information

from many sources in order to provide it to lenders for credit decisions. If the information is incorrect, it may prove to be difficult or even impossible for the consumer to obtain credit even though he or she might otherwise be considered eligible if the information were correct. The Congress, quite understandably, believed that this was of tremendous significance to the consumer. Under H.R. 4585, however, the consumer is to be given access to information whether or not it is used for any purpose whatsoever.

Thus, under the literal language of H.R. 4585, an individual can call any financial institution and demand to see any medical information that might be held anywhere in the institution no matter for what purpose it is held. In fact, the consumer apparently can generate a search even though he or she does not have a basis on which to believe the institution has or is using medical information. In order to comply with such a request, the institution would, under the language of the bill, need to query the great majority of its employees to see if each employee has somehow or other gathered some medical information on the consumer. While this may not have been the intent of the legislation, it is a plain reading of its language.

Part of the problem may be a misconception that there is, in any financial institution, one list that contains all the information about a consumer. In institutions of even the smallest size, that is not the case. At any given time, there are numerous lists, developed under different circumstances or for different purposes. There also is information in many employees' files that is never put on any list or in a database. While it, again, may not be the intent of the legislation, let me cite a few examples that would seem to be covered by the consumer access requirement. Note in this context that the definition of "individually identifiable health information" in the bill is very broad.

First, it would seem that a bank would have to go through every check written by the consumer and every credit card slip in its files to see if they contained any applicable medical information – ***a process that is <u>not</u> done today and is antithetical to the notion of medical privacy***. Such a huge undertaking would necessarily involve speculation on the part of the financial institution as to what constituted medical information. For example, would a debit card transaction at the local CVS pharmacy be considered medical information? Clearly, CVS sells

thousands of products that are not medically related. Moreover, financial institutions would also have to review any loan made to the consumer to see if the proceeds of that loan were, in any fashion, used for medical purposes and the fact that the money was so used somehow communicated to the bank. All lending officers and insurance agents would have to be asked if they had ever taken any medical/insurance information as part of a loan or insurance application and kept that information in one of their files.

The institution would also, under the literal language of the bill, have to query all its branches to see if any information had been provided to branch personnel. This would not be limited to the home branch of the customer, as the customer could have had some interaction with any branch. Suppose, for example, that a customer goes into a branch away from his or her home town for a cash advance on a credit card to deal with the costs surrounding an extended stay due to injury to a family member caused by an accident. Suppose also that the branch manager, in the process of making every effort to aid the customer, recorded in a file the nature of the situation. If, six months later, that same customer calls an 800 number and requests his or her medical information, the bank would be in violation of the law if it did not include the record of that branch manager, even though the home office had no way of knowing that the branch manager had the information or had ever dealt with the customer. Literally, to be in compliance, the home office would have to query the great majority of its employees to make sure that none of them had come into possession of some medical information and had it in a file somewhere.

In this respect, the bill provides for reimbursement of "reasonable" costs. What would be a "reasonable" cost? If a "reasonable" cost is that needed to cover the cost to the institution, which we would argue it should, then it could be very expensive to the consumer to make any such inquiry. That, of course, would make the access requirement of no value. Would "reasonable" include the overhead cost of developing and maintaining a system to reply to such inquiries? If "reasonable" means a few dollars, then financial institutions will lose great amounts on any inquiry. Some may argue that such inquiries would be rare, but the institution would still be required to have an expensive process in place to access the information across its entire operation, no matter how infrequent the inquiries might be. On the other hand, since the bill

allows any "consumer" to make such requests, a large group could demand searches just to hurt an institution.

ABA also is concerned about the paragraph on page 7 of the bill entitled "Restraint on Information Requests." Quite frankly, we cannot understand its effect.

In conclusion, Mr. Chairman, the ABA believes that medical information should only be used for the express purpose for which it is provided and should not be shared without the express consent of the customers. However, the ABA does have serious concerns about the legislative process going beyond medical privacy and about specific provisions of the bill. In particular, the ABA is strongly opposed to the provision which would establish a new, open-ended right to force an institution to search for information wherever it may be in an institution and whether or not it is being used to make a decision of any importance to the consumer. The situation is not analogous to the FCRA, where consumers have a legitimate concern that misinformation in a specific place – a credit file – could adversely affect his or her ability to obtain credit. Under H.R. 4585, there is no requirement that the information is being used in a manner of any importance to the consumer. We hope that these concerns can be addressed by the Committee and we look forward to working with Committee members to that end.

Voluntary Guidelines for Responsible Use and Protection of Customer Information

Introduction

The financial services industry has a long history of using customer information responsibly. The industry values the trust customers have that financial institutions will protect their personal financial information. New technologies have dramatically changed the way information is gathered, used and stored, but the importance of preserving customer trust and confidentiality of personal information has remained a core value of the financial services industry.

This special task force has developed these voluntary guidelines that encourage financial institutions to reassess, through self-examination, how they use customer information. In partnership with their customers, financial institutions reaffirm the strong commitment to safeguard personal information and provide high-quality, affordable and innovative products and services.

This task force consisted of representatives from banking institutions of all sizes and from all parts of the country. It included CEOs, privacy experts, representatives of non-bank affiliates, and third party providers. These guidelines express broad concepts to be followed. They are not meant to provide a detailed, legal explanation covering every possibility — for example, the need to provide information in response to a subpoena, to process an insurance claim, or to market an institution's services or provide products jointly with business partners. Nor do the guidelines constitute a privacy policy, which would need to be more detailed, although these guidelines should serve, along with the legal requirements of the Gramm-Leach-Bliley Act, as the basis of an institution's privacy policy.

5. **Financial Institutions Have Procedures Designed to Maintain Accurate Information**

   Financial institutions have procedures designed to maintain accurate, current and complete customer information. Financial institutions respond in a timely manner to customer requests to correct information.

6. **Financial Institutions Help Protect Customers Against Criminal Use of Their Information**

   Financial institutions help protect customers against, and educate customers about how to protect themselves from, criminal use of their information. Financial institutions use a combination of safeguards to protect customer information, such as employee training, rigorous security standards, encryption and fraud detection. Institutions work with law enforcement officials to pursue individuals who fraudulently use information.

7. **Financial Institutions Have Procedures to Prevent Unauthorized Access to Customer Information**

   Financial institutions maintain security and confidentiality procedures designed to prevent unauthorized access to customer information.

8. **Sharing Information Within the Family of Companies Improves Customer Service**

   Financial institutions share information within their family of companies in order to provide customers with the best possible products and services at reasonable prices, and to prevent fraud and criminal activity. Financial institutions describe the options they make available to customers to provide or restrict information within the family of companies, make it convenient for customers to choose among those options, and honor the choices that are made.

9. **Disclosure of Information Outside the Family of Companies is Restricted**

   If information is provided outside the family of companies for marketing nonfinancial products, financial institutions provide each customer the opportunity to prevent, or opt-out of, the exchange of information. If such information is provided to parties outside the family of companies, financial institutions obligate such parties to adhere to the financial institution's policy that provides for keeping such information confidential, and inform them that it is against the law to disclose such information for any purpose other than that for which it was originally provided.

10. **Account Numbers Are Not Provided Outside the Family Of Companies For Marketing Purposes**

    Financial institutions do not provide account numbers to parties outside the family of companies for marketing purposes.

Voluntary Guidelines for Responsible Use and Protection of Customer Information

Guidelines

1. **Financial Institutions Recognize Customers' Expectations for Responsible Use and Protection of Information and Communicate Their Information Practices to Those Customers**

   Financial institutions recognize and respect the expectations of their customers regarding use of personal information, and provide information to customers on how information about them is used and protected, and the benefits such use provides. Financial institutions provide their customers with their policies on responsible use and safeguarding of information, and provide a means by which customers can learn more about the information practices of their institutions.

2. **Preserving Trust is a Core Value**

   Safeguarding customer information requires standards of conduct for each employee regarding the responsible use and protection of personally identifiable information. Financial institutions educate their employees to respect the importance of maintaining the confidentiality of customer information and take appropriate disciplinary measures to enforce employee responsibilities.

3. **Medical Information Will Not Be Shared**

   Financial institutions recognize that, when consumers provide medical information for a specific purpose, they do not wish it to be used for other purposes, such as for marketing, or in making a credit decision. If a customer provides personal medical information to a financial institution, the financial institution will not disclose the information, unless authorized by the customer.

4. **Responsible Use of Information Provides Customer Benefits**

   Information financial institutions collect provides significant customer benefits. It enables financial institutions to understand customers' financial needs, improve products and services, comply with laws and regulations, provide enhanced customer service, and protect customers against fraud.

Testimony of the

AMERICAN COUNCIL OF LIFE INSURERS

Before the

HOUSE COMMITTEE ON BANKING AND FINANCIAL SERVICES

On

The Medical Financial Privacy Protection Act

June 14, 2000
2128 Rayburn House Office Building

1001 Pennsylvania Avenue, NW - 5th Floor Washington, DC 20004-2599
Telephone: 202/624-2000 Facsimile: 202/624-2319

I. INTRODUCTION

The American Council of Life Insurers (ACLI) is pleased to submit this statement on the Medical Financial Privacy Protection Act (H.R. 4585) to the House Committee on Banking and Financial Services. The ACLI is a national trade association whose 435 member companies represent approximately 73 percent of the life insurance and 87 percent of the long term care insurance in force in the United States. They also represent over 80 percent of the domestic pension business funded through life insurance companies and 71 percent of the companies that provide disability income insurance. The ACLI commends Chairman Jim Leach for calling a hearing on this important subject and for sponsoring this legislation.

II. ACLI POLICY POSITION

Life, disability income, and long term care insurers are well aware of the unique position of responsibility they have regarding an individual's personal medical and financial information. ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. Toward this end, the ACLI Board of Directors has adopted policy in relation to confidentiality of medical and financial information.

ACLI's Confidentiality of Medical Information Principles of Support and Confidentiality of Financial Information Principles Support are grounded in the industry's long history of dealing with highly sensitive information in a professional and appropriate manner. These principles also acknowledge the changing horizon of the financial marketplace. For example, where a bank and an insurer are affiliated, should a bank evaluating an application for a mortgage or credit be able to use medical information from the insurer indicating that a mortgage applicant has a history of heart disease? ACLI member companies strongly believe that the answer to that question - and similar ones - should be a resounding " NO."

We support strict protections for medical record confidentiality, including a prohibition on an insurer sharing medical records with a financial company, such as a bank, for use in determining eligibility for a loan or other credit - even if the insurance company and the financial company are commonly owned. We also support a prohibition on the sharing of medical information by an insurer for marketing purposes. It is our policy that life, disability income, and long term care insurers should not share medical information for marketing purposes, for example, with pharmaceutical companies or drug stores. Copies of the ACLI "Principles of Support" are attached.

The very nature of life, disability income and long term care insurance involves personal and confidential relationships. These insurers must be able to obtain, use, and share their customers' personal health and financial information to perform legitimate insurance business functions. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. ACLI member companies also believe

that the sharing of information with affiliates and unaffiliated third parties generally increases efficiency, reduces costs, and makes it possible to offer economies and innovative products and services to consumers that otherwise would not be available.

LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURANCE POLICIES

The fundamental purpose of life, disability income and long term care insurance is to provide financial security for individuals and families:

- **Life insurance** provides financial protection to beneficiaries in the event of the insured's death. Proceeds from a life insurance policy may help a surviving spouse pay a mortgage or send children to daycare or college.

- **Disability income insurance** replaces lost income when a person is unable to work due to injury or illness.

- **Long term care insurance** helps protect individuals and families from the financial hardships associated with the costs of services required for continuing care, for example, when someone suffers a catastrophic or disabling illness.

Every year America's life, disability income and long term care insurers enter into millions of insurance contracts. Those contracts represent the promises we keep to our policyholders.

III. USE OF PERSONAL HEALTH AND FINANCIAL INFORMATION BY LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURERS

UNDERWRITING THE POLICY

When a consumer begins the search for a life, disability income, or long term care insurance product, he or she often begins by meeting with an insurer's sales representative. Generally, the sales representative will discuss with the individual his or her family's financial security and estate planning goals. If the consumer decides to apply for individually underwritten insurance, the sales representative will complete an application.

Many of the application questions concern nonmedical information, such as age, occupation, income, net worth, other insurance and beneficiary designations. Other questions focus on the proposed insured's health, including current medical condition and past illnesses, injuries and medical treatments. The sales representative also will ask the applicant to provide the name of each physician or practitioner consulted in connection with any ailment within a specified period of time (typically five years).

Up to this point in the process, the information the insurance company receives about the

applicant has come directly from the applicant. Depending on his age and medical history and the amount of insurance applied for, the insurance company may require medical record information or additional financial information. When the sales representative takes the consumer's application for insurance, the agent also will ask him to sign a consent form authorizing the insurance company to verify and supplement the information about him, and to obtain additional information if it is needed to evaluate the application.

The medical information that insurance companies typically request of applicants includes routine measurements, such as height and weight, blood pressure, and cholesterol level. The insurer may also seek an evaluation of blood, urine or oral fluid specimens, including tests for tobacco or drug use or HIV infection. Medical tests are done only with the applicant's consent. Since life, disability income, and long term care insurance policies are long range financial products purchased to provide financial security, it is often necessary for the insurer to also assess and use personal financial information, such as occupation, income, net worth, assets, and estate planning goals.

The price of life, disability income, or long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Life, disability income, and long term care insurers gather this information during the underwriting process. Based on this information, the insurer groups insureds into pools in order to share the financial risks presented by dying prematurely, becoming disabled or needing long term care.

This system of classifying proposed insureds by level of risk is called risk classification. It enables insurers to group together people with similar characteristics and to calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. The process of risk classification provides the fundamental framework for the current private insurance system in the United States. It is essential to insurers' ability to determine premiums which are adequate to pay future claims and fair relative to the risk posed by the proposed insured.

Some individuals are concerned that their medical record information will be "used against them" to deny or cancel coverage, or to increase premiums. In fact, underwriting and the process of risk classification, based in large part on medical record information, have made life, disability income and long term care insurance widely available and affordable: 95 percent of individuals who apply for life insurance are issued policies and 91 percent obtain it at standard or better rates.

Once a life, disability income, or long term care insurance policy is issued, it cannot be canceled for *any* reason except for nonpayment of premiums. Premiums for these types of coverage cannot be raised because an individual files a claim, or because an individual becomes ill after purchasing the policy. However, if an individual suffers from a serious medical problem at the time a life insurance policy is issued, the premium may be reduced in some cases when the insured's health improves. Also, although premiums for some disability income or long term care insurance policies may be increased based on macro-economic factors, they may never be

increased on an individual basis. Disability income and long term care insurance premiums may only be increased for a whole block of policies, usually only to ensure that premiums are adequate to pay claims.

THE BUSINESS OF LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURANCE

Once a life, disability income, or long term care insurer has an individual's personal health and financial information, the insurer limits who sees it. However, the insurer must use and share that information to perform legitimate, essential insurance business functions – to underwrite the applications of prospective customers, as described above, to administer and service existing contracts with consumers, and to perform related product or service functions. Life, disability income, and long term care insurers must disclose personal information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals (such as the detection and deterrence of fraud). Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' sharing of personal information.

PERFORMANCE OF ESSENTIAL INSURANCE BUSINESS FUNCTIONS

Many insurers use affiliates or unaffiliated third parties to perform all or part of the essential, core functions associated with an insurance contract. It is quite common for these insurers to use affiliates or third parties to perform basic functions such as underwriting, claims evaluation, and policy administration. In addition, insurers also use third parties to perform important business functions, not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, development and maintenance of computer systems.

Third parties, such as actuaries, employee benefits or other consultants, physicians, attorneys, auditors, investigators, translators, records administrators, third party administrators, and others are often used to perform business functions necessary to effect, administer, or enforce insurance policies or the related product or service business of which these policies are a part. Often these arrangements with affiliates or unaffiliated third parties provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.

If an individual were to be permitted to withhold consent for a life, disability income, or long term care insurer to share his or her personal information with an affiliate or a third party performing a core insurance business function for the insurer, it would be extremely difficult, if not impossible, for the insurer to provide that consumer with the coverage, service, benefits, or economies that otherwise would be available. For example, suppose an individual seeks life insurance coverage from an insurer which uses an affiliate or a third party to do its underwriting. If the individual withholds or subsequently withdraws consent for the insurer to divulge his personal health information, the insurer either cannot underwrite the policy because it does not

have the internal capacity to do so or it must create a special system to accommodate this one individual.

DISCLOSURES PURSUANT TO REGULATORY/LEGAL MANDATES OR TO ACHIEVE CERTAIN PUBLIC POLICY GOALS

Life, disability income, and long term care insurers must regularly disclose personal health and financial information to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information. Any limitation on these disclosures would seem likely to operate counter to the underlying public policy reasons for which they were originally mandated – to protect consumers.

Life, disability income, and long term care insurers need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, which work for the insurer. Any limitation on insurers' ability to make these disclosures would seem likely to undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.

The continued ability to make disclosures to the MIB is essential to insurers' efforts to combat fraud, yet it often comes under attack. The purpose of the MIB is to reduce the cost of insurance by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. A provision permitting individuals to withhold consent for insurers to make disclosures to the MIB would require the insurance industry to abandon this effort at combating fraud and abuse. It would be like asking a bank not to do a credit check before it issues a mortgage. The result would be higher costs for all consumers.

ORDINARY BUSINESS TRANSACTIONS

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Naturally, these files can contain personal information. Such disclosures are often necessary to the due diligence process which takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly created entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements often

necessitate the disclosure of personal information by the primary insurer to the reinsurer. Depending on the particular reinsurance treaty, this might happen because the reinsurer: (1) wishes to examine the ceding insurer's underwriting practices; (2) actually assumes responsibility for underwriting all or part of the risk; or (3) administers claims.

If an individual insured were to be permitted to withhold or withdraw consent for an insurer to disclose personal information in situations where the sharing of that individual's file is necessary to a merger, acquisition, or reinsurance arrangement, that individual could hold hostage or prevent a transaction likely to benefit hundreds, or possibly thousands, of other policyholders. This would deprive other policyholders of the economies and product opportunities for which the transaction was originally sought.

IV. SPECIFIC COMMENTS ON H.R. 4585

As you know, Title V of the Gramm-Leach-Bliley (GLB) Financial Services Modernization Act signed into law last year provides American consumers with the most comprehensive financial privacy protections in the nation's history. Under the GLB Act:

> Every financial institution is required to disclose to consumers its policy and practices designed to protect the confidentiality and security of personal financial information at the start of a business relationship, and at least once each year for the remainder of the relationship.
>
> Every financial institution is prohibited from disclosing account numbers to unrelated third parties for use in direct marketing, telemarketing, or marketing through e-mail to consumers.
>
> Consumers have the legal right to say no or to opt-out of the disclosure, transfer or sale of their personal financial information to unrelated third parties, unless the disclosure is to a service provider, pursuant to a joint agreement between financial institutions, or for an ordinary business purpose.
>
> It a federal crime to obtain private personal information from a financial institution under false pretenses.

We appreciate that the bill under consideration today follows the framework of the GLB Act. It appropriately seeks to balance consumers' confidentiality requirements with financial institutions' need to disclose medical information, like financial information, in order to perform ordinary business functions. However, we believe that the bill fails to achieve this balance. We are concerned about several provisions of the legislation.

GLB ACT EXEMPTIONS

The bill fails to include several of the key GLB Act exemptions. GLB Act Section

502(b)(2) provides an exemption for financial institutions' disclosures to nonaffiliated third party service providers. Section 502(e) exempts disclosures to nonaffiliated third parties performing ordinary business functions for the financial institution. It is absolutely critical that the same exemptions be provided with respect to disclosures of individually identifiable health information as have been provided with respect to disclosures of financial information. Otherwise, insurers' ability to service their existing and prospective customers will be significantly jeopardized.

The bill does not provide an exemption for disclosures by a financial institution to nonaffiliated third parties performing services for, or functions on behalf of, the financial institution. As a result, every day communications between an insurer and its third party contractor agents would be hindered. These communications are often essential to an agent's ability to best advise a prospective customer with respect to which insurance policy (or policies) may be best for his or her particular circumstances.

The bill also fails to follow the GLB Act by not including exemptions for disclosures to state guaranty funds or disclosures governed by the federal Fair Credit Reporting Act (FCRA). It would seem to be contrary to the public interest to hinder disclosures to state guaranty funds which seek to pay consumers' claims in the event of insurer insolvencies. Moreover, given the GLB Act's explicit language preserving the FCRA, it is unclear why the GLB Act exemption for disclosures governed by this Act has not been included.

In view of the above, the ACLI strongly urges that the bill be amended to include *all* the GLB Act exemptions. In this event, the bill still would address consumers' confidentiality concerns relating to their individually identifiable health information without unnecessarily jeopardizing insurers' ability to best serve consumers which come to them for insurance products and services.

RIGHTS TO ACCESS, CORRECT, AND AMEND

Section 2(c) of the bill would grant consumers an extremely broad right to access and correct individually identifiable health information held by financial institutions. The bill fails to clearly protect from this access information compiled in anticipation of or in connection with an investigation of fraud or material misrepresentation. It also fails to clearly protect information gathered in connection with legal proceedings. This would seem to be counter to the public interest. The ACLI strongly urges amendment to clarify and appropriately limit this access to that which meets consumers' legitimate needs and concerns without needlessly jeopardizing a number of public policy goals.

SPECIAL REQUIREMENT TO PROTECT MENTAL HEALTH INFORMATION

The bill provides special protection for mental health information. Section 3(a)(3)(A) requires that the regulations issued to carry out this Act include special policies and procedures to protect the confidentiality of mental health information. We are concerned that requiring "special procedures" with regard to mental health information will result in the segregation of

this information that could jeopardize a life, disability income, or long term care insurer's access to this information. Insurers must be able to access medical information relevant to the underwriting and claims processes. Without access to relevant medical information existing at the time of application, the insurer cannot accurately calculate risk. This could result in premiums that do not fairly reflect the level of risk presented by individuals, resulting in adverse selection. Similarly, without access to relevant medical information during the claims evaluation process, an insurer will have no way to determine its obligation under an existing insurance contract.

Section 2(a), amending the Gramm-Leach-Bliley Act at 502(A)(d) requires a *separate* and specific consent for mental health information. A major objective of the proposed legislation is to provide individuals with greater control over their protected health information. This can be achieved without imposing unnecessary burdens on the financial institutions that would be governed by the Act. Given adequate notice regarding mental health information, there is no reason to require a separate authorization for this medical information. Mental illnesses are real, diagnosable, and treatable. The rules governing the privacy of medical information should apply equally to all medical information. Thus, the ACLI strongly urges that the bill be amended to delete the proposed requirements for special policies and procedures and separate consent in relation to mental health information.

PREEMPTION

The ACLI supports the principle that in the event federal medical privacy legislation is considered by Congress, that legislation should preempt related state laws. Life, disability income and long term care insurers engage in interstate commerce — their customers should know that health information disclosed by these entities is governed by the same standards of protection, regardless of their location. This bill, unlike the comprehensive medical information privacy bills, deals exclusively with financial institutions. The issues surrounding preemption that stalled the debate on comprehensive legislation, including the possible preemption of state parental notification laws, do not exist in this legislation. Thus, there is no reason for this bill not to clearly preempt state laws in this area.

V. CONCLUSION

It is imperative that any debate in relation to medical records privacy be thoughtful and not political. We have grave doubt that thoughtful debate is possible at this time in the highly politicized environment of an election year. Any legislation in relation to this issue must reflect a careful balance of consumers' confidentiality concerns with consumers' insurance needs. No medical records privacy bill should jeopardize the current life, disability income, and long term care insurance marketplace which meets consumers' insurance needs. No medical records privacy bill should jeopardize insurers' ability to underwrite, process claims, and perform other core or ordinary insurance business functions.

We appreciate that certain provisions, found in the comprehensive health information privacy bills, which could significantly jeopardize the current life, disability income or long term

care insurance marketplace, have not been included in this measure which focuses exclusively on financial institutions. We strongly urge that the exceptions outlined in the GLB Act that were not included in this legislation be restored. Finally, we also strongly urge you not to raise issues that have been divisive in other medical privacy debates, namely third party liability issues under a "business partners" concept, and excessive damages awards, including punitive damages.

Again, the ACLI greatly appreciates your leadership, Chairman Leach, on this issue so important to American consumers and those who serve them. This industry has a long history of dealing with medical information in an appropriate, confidential fashion. Over the past 200 years, we've earned the trust of our customers. And we intend to keep it.

Confidentiality of Financial Information

Principles of Support

Life insurers provide financial security for millions of Americans through life, long-term care, and disability income insurance and annuities. To enable companies to provide products that meet an individual's or family's unique needs, insurers ask questions and collect financial information.

Life, disability income and long-term care insurers recognize consumers are concerned about revealing financial information. They want to know how the information will be used and who will have access to it. Life insurers should have policies and practices that address these concerns and protect confidentiality.

Insurance companies strongly support the following principles, which require financial information to be treated confidentially.

Separate Principles for Medical and Financial Information

Life insurers recognize that customers have special concerns regarding medical information. Therefore, insurers have separate policies and practices for securing the confidentiality of medical information.

Strict Policies and Practices to Protect Financial Information

An insurer will have policies and practices in force to protect the confidentiality and security of financial information. These policies and practices are designed to protect the information from unauthorized access and use so that customers are not substantially harmed or inconvenienced.

Customer Notification of Confidentiality and Security Policies

Customers will be notified of the policies and practices an insurer follows to protect the confidentiality and security of their financial information. The insurer will give customers a notice of its policies and practices before or at the time a contract is issued, and after that on an annual basis, for as long as the contract is in force.

Customer Access to Financial Information

Upon request, customers are entitled to have access and correction rights to their financial information collected in connection with an application for life, disability income, and long-term care insurance and annuities.

Limitations on Sharing Financial Information

An insurer may share financial information to issue contracts and to administer and service its

business. For example, an insurer may share financial information to facilitate paying claims, provide consolidated financial statements of a customer's accounts, prevent fraud, or comply with the law.

An insurer may share financial information only with organizations that are subject to the same restrictions on information sharing as the insurer.

Strict Rules on Sharing Financial Information for Marketing Purposes

An insurer's notice of policies and practices about financial information will inform customers that the information may be shared for marketing products and services consumers may find useful. For example, an insurer may share financial information within its corporate family, with a financial institution with which it has a joint agreement, or with an organization responsible for marketing the insurer's products and services.

The insurer will give customers the opportunity to direct that financial information not be shared if the products and services being marketed are not offered through the insurer's corporate family, through a joint agreement with another financial institution, or by an organization marketing the insurer's products and services.

Confidentiality of Medical Information

Principles of Support

Life, long-term care and disability income insurance companies recognize an individual's medical information is personal, sensitive and must be protected. Companies have policies and practices in place to protect the confidentiality and security of an individual's medical information, and individuals have a right to have information about those policies and practices.

Insurance companies strongly support the following principles, which require individually identifiable medical information to be treated confidentially.

Strict Restrictions on Obtaining Medical Information

- Medical information will not be collected without an individual's authorization in connection with an application for life, long-term care and disability income insurance.

Strict Ban on Sharing Medical Information for Marketing

- Medical information will not be shared for marketing purposes.

Strict Ban on Sharing Medical Information with Other Financial Companies

- Under no circumstances will an insurance company share an individual's medical information with a financial company, such as a bank, in determining eligibility for a loan or other credit – even if the insurance company and the financial company are commonly owned.

Strict Restrictions on Disclosing Medical Information

- Any disclosure of medical information without an individual's permission will be made only in limited circumstances as authorized or required by law. For example, information may be disclosed to facilitate paying claims, and to state insurance commissioners enforcing consumer protection laws.

- Disclosures of medical information will contain only the information authorized by the individual or authorized or required by law. The recipient of the information should be subject to the same confidentiality standards as the insurance company.

- The insurance company must inform an individual, upon request, what medical information has been disclosed and to whom it has been disclosed.

- An individual may sue for actual damages if an insurance company improperly discloses personal medical information.

Strict Confidentiality Policies and Practices

- Life, long-term care and disability income insurance companies must document their confidentiality policies and practices, and adopt internal operating procedures to restrict access to medical information.

- An individual is entitled to receive information describing the insurance company's medical information confidentiality policies and practices.

- Upon request, an individual is entitled to access medical information collected in connection with an application for life, long-term care and disability income insurance and to obtain correction of inaccurate medical information.

Uniform Confidentiality Protection

- State legislation seeking to implement these principles should be uniform. Any federal legislation seeking to implement the principles should preempt all state requirements relating to the confidentiality of medical information.

Testimony of

Nicole Beason

Esther Peterson Fellow
Washington Office
Consumers Union

Before the

House Committee on
Banking and Financial Services

On

The Medical Financial Privacy Protection Act

June 14, 2000

Consumers Union[1] (CU) appreciates the opportunity to testify about medical and financial privacy protection, and the sharing of medical information. CU has advocated for medical privacy for many years. We recently filed comments with the Department of Health and Human Services on their proposed rule for Standards for Privacy of Individually Identifiable Health Information.

Consumers Union believes that any legislation on medical privacy should provide consumers (1) with the right to amend and/or correct their health information records; (2) have access to their medical records, and decide whether to release individually identifiable medical or financial information, the "opt-in" approach. We also believe that health care providers, financial institutions and other holders of health and financial information have a duty to maintain the confidentiality of individually identifiable health information and should be held accountable for protecting an individual's privacy interest. Because H.R. 4585 addresses these issues, Consumers Union supports Chairman Leach's legislation, but believes it should be strengthened.

Americans support strong federally mandated protections for the privacy of individually identified health information. In 1993, a Lou Harris poll found that 97% of those who were surveyed believed that protecting their medical privacy was important, and 36% found that it was absolutely essential. Another poll showed that 96% of

---

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

Americans believed that rules should be implemented to state which individuals have access to medical records and the information that they can obtain. My testimony today will focus on issues that are of primary concern to consumers -- notice and consent, sharing of information within multi-business corporations, and the ability to amend and correct their information.

The bill provides that a financial institution may not disclose any consumer's individually identifiable health information unless it has provided clear and conspicuous written notice, an opt-in measure for consumers, and has obtained written consent by the consumer that has not been withdrawn. Consumers should be given written notice in plain language of how their individually identifiable health information will be used and by whom. This notice should explain which information will be collected, for what purpose it will be used, how it will be protected, and the consequences of providing or withholding requested information.

Individually identifiable health information provided to a financial institution by a consumer should not be transmitted to anyone else including affiliates and third parties without the consumer's informed consent. The fact that the bill provides that consumer consent has to be given before the release of private health information can be made is of utmost importance. Personal information should not be shared unless consumer authorization has been secured for a specific use. There should also be special procedures implemented for those who are disabled. This is important in such cases where a disabled person is incapable of giving written consent. There needs to be procedures in place to allow a fiduciary to act on the individual's behalf. This "opt-in"

measure affords greater privacy protection for consumers because it allows them to give informed consent to share their highly sensitive health information before that information can be shared by financial institutions.

To protect medical privacy, it is important that the "opt-in", which waives the privacy interest, should be clear. Because consumers may never read these broad forms, specific disclosures need to be given regarding medical privacy. General, boilerplate consent forms, which contain provisions that allow private information to be dispersed to a broad range of entities deserve scrutiny.

In addition to covering the sharing of information with third parties, this bill extends those protections to the sharing of information with affiliates. This makes clear the intent of the bill is to ensure that health information is not shared with any other party without the consumer's consent. Many consumers do not understand the distinctions between affiliates and third parties. Financial institutions, especially in the aftermath of financial modernization, may consist of a family of companies. Those companies may offer everything from insurance to investment products. If the bill did not cover affiliates, health information could be shared throughout all these companies and could be used inappropriately.

The bill provides that a financial institution shall amend, correct, or delete material information identified by a consumer that is materially incomplete or inaccurate, or shall notify the consumer of its refusal to do so. In doing so, the institution must give reasons for its refusal, the identity of the entity that created the information, and refer the consumer to that person in order to amend or correct the information, or file a statement of what the consumer believes should be the correct information.

Consumers should have the right to ensure the accuracy of their own health information. Consumers should also have the ability to amend and correct inaccurate information. Should a consumer consent to sharing their health information, inaccurate information may have serious consequences for them. For example, they could be declined insurance coverage because their records falsely indicate that they have a poor medical history. Therefore, it is important that a proper system be implemented to allow consumers to amend and/or correct any mistaken or inaccurate information. It is also important for the consumer to receive notice of any refusal and the identity of the original creator of the disputed information.

The Fair Credit Reporting Act can serve as a model for the regulators to use to implement this requirement. Specifically, we are concerned that one of parties who has a vested interest in this information is not allowed to make a blanket determination as to whether the disputed information is included or shred with other parties. Though the bill allows a consumer to receive information about the original creator of the disputed information, covered entities may not implement full and fair procedures to handle discrepancies in individuals' medical records. They should not be allowed to automatically deny a consumer's request to amend and correct medical information. The FCRA provides a proper framework for giving consumer's the ability to amend and correct inaccurate information, because it provides a heightened standard of fairness.

We believe that the FCRA is relevant in this context because it governs the accuracy of information contained in financial records, the importance of which is similar to medical information. Therefore, medical records should be afforded, at a minimum, the same level of protection that is given to financial records under the FCRA.

There are additional concerns about H.R. 4585 that we share with other consumer advocates. The exceptions, if any, should be limited. The bill should not contain any loopholes that would allow financial institutions to share a consumer's medical information counter to the intent of this bill. Also, a financial institution should not be allowed to use health information about a consumer without the consumer's consent, not just for decisions regarding a loan or credit, but for any product or service offered by the institution to the consumer. We are also concerned about health information that may already be in the financial institution's possession. If the intent of this bill is to stop information sharing, then it should apply prospectively to information that banks have already obtained.

Consumers Union appreciates the opportunity to testify on this important issue. Consumers care about the privacy of their health information and this bill will help to protect that information when dealing with increasingly complex transactions in the financial services industry.

Testimony
of

A.G. Breitenstein, JD, MPH
Chief Privacy Officer
ChoosingHealth.com
(617) 283-8483
ag@choosinghealth.com
29 Forest St. #2
Somerville, MA 02143

Regarding
H.R. 4585

Before
House Committee on Banking and Financial Services

The Honorable Rep. Leach
Chairman

Good morning, Chairman Leach and members of the committee. Thank you for inviting me here to testify before you on this very important issue of the privacy of personal health information.

Let me introduce myself. My name is A.G. Breitenstein. I am the Chief Privacy Officer of a young Internet startup company known as "ChoosingHealth.com." ChoosingHealth is the first Internet service of its kind to allow patients to communicate with other patients and with researchers, hospitals, doctors, pharmaceutical companies and other health industry vendors without having to give up their privacy. We are dedicated to the notion that a patient's health information belongs to them and is one of the most valuable resources that exists in our burgeoning information age.

I particularly want to thank you for taking up this very important and very challenging issue. A Wall Street Journal Poll recently found that Americans consider the issue of health privacy to be more threatening than domestic terrorism. A 1999 Harris Poll found that Privacy was the number one reason why individuals are choosing to stay off of the Internet. And as we have seen to date, few legislative or regulatory solutions have succeeded in properly addressing this issue.

But the urgency of this problem is clear. In the discussions that I have had with health care practitioners, the current lack of patient confidentiality has already had a profound impact on the way in which they practice medicine. Dr. Nancy Dickey, past President of the AMA, has stated that "these days insurance companies don't want summaries; they want the whole record. So I think twice about what I include. Then I hope that I can remember it all...If my patients fear that what they tell me could comeback to haunt them, they'll tend to be less forthright. I may come up with the wrong treatment because I was chasing the wrong clues."

Dr. Dickey is not alone. I once spoke with one physician who reported to me that his wife, also a doctor, routinely "doodled" in the margins of her medical records. And that her doodles were, in fact, coded messages to herself regarding her patient's medical histories. She felt the need to protect this information because these records are routinely sent to insurance companies and often accessible to employers and others. She was rightly concerned, however, that the care of her patient might be compromised if anything happened to her and no one was able to decipher her doodles.

This dramatic loss of privacy has been made worse by the increasing demands of the "health care system" for information that was previously held within the one-on-one doctor-patient relationship. As Dr. Ricardo Lewitus a pediatrician has stated:

> Insurance companies are requesting us as part of 'well visits' to ask and document (which I have no problem with) questions such as: Do you have sex? Do you masturbate? How are your relationships with your parents, friends? Have you had an abortion? And many others. As I said, I have no problem asking these questions. What disturbs me is the access that insurance companies have to that information and therefore anybody else that wants or can legally obtain those records. We physicians are in a Catch 22. If we document, patient confidentiality can be destroyed; if we do not document then we are classified as 'bad doctors.' As a pediatrician, I am very concerned about how information available to third parties will affect these children's futures.

These stories show us that patients are being forced into an awful choice between their health and their privacy. For many, especially those with HIV, mental illness, genetic disorders, etc, this choice can be gut wrenching and destructive. Your efforts here in legislating this issue will have a profound impact on the integrity and effectiveness of the health care system as well as the personal integrity of each and every one of us. I am here before you today to support you in your efforts to protect this valuable and common resource we now know as our health privacy. The proposed legislation is a good first step. I would like to commend you for tackling this issue and to make a few suggestions for improvement. I am also here to give you some sense of how your efforts in this effort are going to shape the future of health privacy, health care and the wider realm of personal identity in the new economy.

If there is one thought that I would like you to take away from my testimony today, it is this one: **Personal information, particularly health information, is the new cash in the digital age. Your efforts to protect the privacy of personal health information will set the terms that will allow individuals to negotiate on a level playing field for the value of this new currency. Without adequate protections individuals will be robbed of a valuable resource and will be reluctant to purchase the goods and services they need.**

What do I mean by this statement? It will help to make a few observations.

1) **When people get stuff for "free" in our new digital economy, they are generally paying for things by giving up some amount of personal information.** This is particularly true on the Internet. E-commerce sites have learned quickly that they can offer "free" goods and services by collecting vast amounts of personal information like buying habits, profiled interests, etc, and selling them to others. Most websites have either as their primary or

secondary source of revenue, some plan to sell personal information. In this way, our personal information is used as a stand-in for cash.

2) **Personal health information is the most valuable of all of the various categories of information, followed closely by one's financial information.** As such, health and financial information are the most valuable of all the bits of personal data that can be collected. They are also the hardest to acquire. If, for instance, a bank has data from the purchase of an inhaler for my asthma, the fact that I have asthma is significantly more valuable than the $10 transaction involving the inhaler. If I, as a bank, can collect and sell a list of people who have asthma to an unscrupulous researcher or a direct marketer I can make millions of dollars. Similarly, information regarding my breast cancer diagnosis can be incredibly valuable with regard to my credit worthiness for a home mortgage.

How should these observations affect your work on HR 4585? Let me suggest the following. Privacy legislation will be the backdrop against which the emerging digital economy will be set. It will have a profound influence on the ability and right of consumers to negotiate the value of their personal information in exchange for those goods and services they desire. You are, in effect, creating a new currency of sorts. This is a very subtle, but very radical idea. Your efforts here must incorporate this fact and be vigilant in the protection of personal health and financial privacy. Let me make a few suggestions and observations:

1) **The basic rule of consent must be clear and unambiguous with few exceptions and full information.** Consent establishes the right of the individual not to be robbed of their personal data. If we are venturing into a new information age, we must protect the ability of the individual to protect his/her resources in this realm.

2) **Health information collected for one purpose cannot be used for another purpose without consent.** If I use a debit card to purchase an asthma inhaler, I have done so for the limited purpose of paying for the inhaler. Any other uses that I do not consent to rob me of the value of this personal information. Think of it as a stock certificate that I place in a safe deposit box. Just because I place that information in the bank's custody does not allow that bank to treat it as its own. Secondary uses of that information without my consent should be prohibited, particularly when those secondary uses could affect my access to things like access mortgages, loans etc.

3) **As the banking and insurance functions begin to merge it is going to be exceedingly important to build a fire-wall between these two areas.** People should not be forced by virtue of the privileges we as a society have granted corporations to choose between their health and their ability to own a home or a car. If the insurance side of a business is aware that I have been diagnosed with breast cancer, the banking side should not then be allowed to bar my ability to get a home mortgage.

4) **Individuals must have a private right of action to enforce their claims on their personal health information.** Data is property. If there is one thing we have historically protected in this country, it is the right of an individual to protect his/her property. The failure to do so here will not only adversely affect health care, but will also set a dangerous precedent in the new information era. You will make individuals into helpless dependents upon the state for protection of one of the most valuable resources in our new economy. I cannot stress how pernicious this will be to our fledgling Internet economy.

Let me close by saying this. Many of my esteemed colleagues will testify today that privacy protections are going to drive up costs and stifle economic growth. I want to challenge their argument head on. Personal information is a resource. It has value and as our economy shifts to an information based system, it will become one of the most valuable resources in the world. If we rob individuals of their data, we render them penniless and powerless to participate freely and fairly in a new free market. We will first feel this in rising health care costs owing to an eroded doctor-patient relationship. We will then feel the effects when people offer erroneous information or worse choose not to participate at all. We are already seeing evidence that this is occurring. A 1999 Consumers League study found that 70% of people were unwilling or reluctant to divulge personal or financial information on-line. A 2000 CyberDialogue poll found that 40% of women who have never made a purchase online cited privacy, security and a lack of regulation as the major barriers. Without adequate privacy protections, we will stifle this exciting new driver of our economic growth. I urge you to make this bill as strong as possible and to give the people of this country the right to control the data that is a reflection of their most intimate selves and that will represent them in the new digital economy.

Thank you for your time today. I look forward to working with you on this important legislation and would be happy to offer any help I can.

PRIVACY TIMES

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The House Committee on Banking & Financial Services
June 14, 2000

Mr. Chairman, thank you for the opportunity to testify before the Committee. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 23 years, I have studied, reported on and published a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

Mr. Chairman, I am particularly heartened by your continued leadership on privacy, as you are consistently willing to give the issue a fair hearing. It was through this Committee that amendments to the Fair Credit Reporting Act were passed. And it was you who took the lead in tackling the difficult problems posed by the underworld of "information brokers" who specialize in stealing individuals' confidential information, resulting in important legislation. These were all bipartisan efforts that also would not have been possible without the leadership of the Committee's Ranking Minority Member, Congressman John J. LaFalce. I've seen first hand how Americans have benefited from your cooperative approach to privacy.

Today's hearing represents another advance, as we focus on the vital issue of financial institutions' use of medical data. To me, the issue is not whether overall, HR4585 is a good bill. For the most part, it is. The more important question is whether the Committee should devote its valuable resources to such a narrowly targeted bill at a time when there are many broader privacy issues that need to be addressed. I favor a broader approach.

The Bill

The legislation (HR 4585) is an excellent starting point because it is based upon the standard which must drive all privacy law: affirmative, informed consent. Specifically, it requires financial institutions that include insurance companies, insurance agents and other financial firms which possess individually identifiable health information to obtain a consumer's affirmative consent before sharing that information with an affiliate or a non-affiliated third party. This is the correct standard because Americans generally don't differentiate between affiliates or outsiders. However, they are concerned when information they give for one purpose is used for other purposes without their informed consent.

The measure generally requires consent before a financial institution could use health information in deciding whether to issue credit. The measure would bar financial institutions from requiring consent for obtaining health data as a condition of providing a loan or credit.

Another positive feature of the bill is that it gives consumers a right of access to their medical data, and a right to dispute the accuracy of that data. These are fundamental rights that are essential to privacy protection.

The bill's language needs to be tightened to ensure that some kinds of "consent" do not become mandatory. For instance, would not want a privacy bill to authorize a lender to access the medical database of its life insurance affiliate through some sort of blanket consent form. If you've ever read the consent forms typically used in insurance, banking and employment, you understand that this is a real danger.

Another problem is the limitation of coverage to "loan or credit" granting. This leaves open the possibility that medical information held by financial institutions could be used for marketing, pre-screening and employment.

A Broader Approach Is Needed

Given the limited scope of HR 4585, and the need to protect privacy of all kinds of financial information, I strongly urge the Committee to use the Clinton Administration's financial privacy legislation, introduce in the House by Rep. LaFalce, as the starting point. This bill better addresses the broader issues of financial privacy that were not adequately addressed by last year's Gramm-Leach-Bliley Act.

A Blueprint For Protecting Privacy In America

Privacy is inadequately protected in the United States because of major gaps in our national laws. The traditional approach has been to introduce narrowly tailored privacy bills has specific problems are identified. This has left us with a hodge-podge of privacy laws, such as the Fair Credit Reporting Act, the Cable Television Privacy Act, the Video Rental Privacy Protection Act, the Telephone Consumer Protection Act and the Gramm-Leach-Bliley Act, to name a few.

However, the United States still does not have national laws protecting the privacy of retail and Internet records, medical records and many kinds of financial and insurance records. Considering that we are in an "Age of Convergence," in which various mediums like Internet, cable, communications, banking and wireless data systems are converging, this approach is no longer tenable.

The most effective way to achieve the much needed, more comprehensive approach is for the Administration to propose a national legislative privacy package, and to set up "privacy infrastructure." Then the appropriate Congressional committees would be responsible for acting upon the parts of the package that come within their jurisdiction.

A major problem has been that this Administration, like others before it, has refused to do its part in presenting to Congress a national legislative package. In this Administration, much of the blame for this falls on the U.S. Department of Commerce, which has continued to rely on industry self-regulation long after such an approach has proven ineffective and unworkable. On the issue of privacy, the Commerce Department has an inherent conflict of interest and should get out of the privacy policy business altogether.

The good news is that the Administration is finally moving to fulfill its obligation, albeit in fits and starts. (Better late than never.) As mentioned, the Administration has proposed more comprehensive legislation to protect financial privacy, fulfilling its promise to revisit privacy after the enactment of Gramm-Leach-Bliley.

The Federal Trade Commission has recommended national legislation to protect Internet privacy. The Department of Health & Human Services, due to Congressional inaction, has proposed rules to protect medical privacy. To its credit, HHS has recognized the limits of its rulemaking power, when compared to legislation.

What is also needed is what all other Western nations have: An Independent Office of the Privacy Commissioner. In the U.S., such an office could do the examine the hodge-podge of privacy laws and recommend to Congress how to bring them in line so there would be greater consistency – a level playing field for Americans and the organizations that handle their data.

A Privacy Commissioner would also serve a public resource and an Ombudsman for Americans. Such an office was proposed in legislation introduced during the 1990s by Sen. Paul Simon.

It's important to note that the American public has made it clear that privacy is a priority, and that they want legal protection for their personal data. A wide array of opinion polls consistently confirm broad public support for the kind of national privacy policy that I have outline here.

That is why, I believe, at this point in history, it would not be appropriate to invest scarce Congressional resources in narrowly tailored legislative proposals that fail to address the broader concerns of the American public.

Finally, it is time that all parties recognize that the failure to protect privacy adequately is hurting prospects for e-commerce. Studies show that significant portions of the public are reluctant to engage in e-commerce because of privacy concerns. Moreover, they show that a majority of Internet users who begin to buy online actually abandon their "shopping carts" when they are asked for their credit card numbers. The moral of this story is clear: E-commerce cannot be successful without consumer confidence; and without privacy, there will not be consumer confidence.

By far, it's not too late to solve this problem. It will take a thoughtful mix of legislative and technological solutions to create a pro-privacy environment in which e-commerce can flourish.

But if we fail to undertake these steps, the next debate could, unfortunately, be over "Who Lost E-Commerce."

Again, Mr. Chairman, thank you for this opportunity. I would be happy to answer any questions.

Testimony Of
U.S. Public Interest Research Group

On HR 4585, the Medical Financial Privacy Protection Act
Before the Committee on Banking and Financial Services
Honorable James Leach, Chairman
14 June 2000

by Edmund Mierzwinski
Consumer Program Director, U.S. PIRG

Mr. Chairman, Ranking Member LaFalce, members of the committee: Thank you for the opportunity to testify before you on the important topic of health and financial privacy. My testimony today is on behalf of the U.S. Public Interest Research Group (U.S. PIRG).[1]

We want to commend the Chairman for introducing legislation that would improve the privacy provisions of Title V of the Gramm-Leach-Bliley Financial Services Modernization Act (the Act). As you know, our organization is troubled[2] that, last year, when Congress enacted HR 10/S 900 into law as the Act, it failed to adequately take into account the consumer need for strong privacy protection based not only on notice, but on all of the Fair Information Practices.[3] The chairman's bill, HR 4585, The Medical Financial Privacy Protection Act, is designed to address one of the most important problems left unaddressed in Title V—protecting medical financial privacy.

Summary

We are pleased that the coverage of HR 4585 is very similar to the medical privacy provisions of the Administration's proposal, HR 4380, as introduced by Ranking Member LaFalce, Mr. Markey and others. Nevertheless, while we generally support HR 4585 with modifications as discussed below, we would respectfully point out that we believe that the more comprehensive proposal offered by the President, with amendments, should be the one enacted by the Congress.[4] HR 4380 addresses not only medical financial privacy, but also closes the affiliate sharing and joint marketing loopholes in Title V and makes other important changes that apply not only to medical information, but also to financial information.

By carving out the nearly consensus issue of protecting medical financial privacy, which even the banks are afraid to oppose too strongly, we fear that our task in enacting the balance of the missing privacy elements in the Act will grow even harder. Nevertheless, we commend the Chairman for taking an important step to protect medical financial privacy and urge him to consider adopting strengthening amendments to broaden the effect of his important bill by picking up more pieces of the comprehensive plan proposed by the President. We believe that the public concern for privacy deserves as broad and rapid a response as possible. The need to move quickly has been exacerbated by passage of the Act, which will encourage even more affiliations and more information sharing.

Key Elements of HR 4585 and Suggestions To Improve HR 4585 And HR 4380

Like the President's proposal, HR 4585 recognizes that medical financial privacy deserves the strongest possible protections. Firms would be generally prohibited from sharing health information

without express opt-in consent. Further, several elements of the Chairman's bill infer a very high standard of express consent before sharing, notably its provision that use of information already held requires consent and its provision that mental health information be subject to special separate consent. These are important provisions.

We would suggest that the following amendments to either the Chairman's bill, the President's bill, or both. In addition, we have discussed the bill with the American Civil Liberties Union, the Georgetown University Health Privacy Project and Consumers Union, and associate ourselves with their remarks on other aspects of the bills that need strengthening.

Exceptions: First, both bills have broad exceptions provisions. We believe that there may not be adequate public policy justification for all of the exceptions sought and would urge the committee to carefully reevaluate each of the uses that have been proposed to be exempt from the privacy protections of the two bills.

Non-Coercion/Boilerplate Consent: We believe that consent is a necessary but not sufficient condition for obtaining and using medical financial information. Section 4 of HR 4380 establishes that all consumers be treated equally, whether they are customers of an affiliate or not. The Chairman's bill appears to have a parallel provision, although its construction is somewhat different. Both bills may have useful elements that should be incorporated into a strong final provision. However, neither bill has the additional provision common to the strong medical privacy bills introduced in this Congress—an express requirement that no treatment be conditioned upon provision of consent.

"Loans or Credit:" Important parts of the Chairman's bill restrict its applicability to the provision of "loans or credit" but not to other products and services offered by or anticipated to be offered by either the one-stop financial supermarkets or their joint marketing partners enabled by the Act. The protections of any medical financial privacy bill should apply across the board, to the use of medical privacy information for any purpose. Under the limitation to "loans or credit," sensitive medical information could be used for pre-screening, marketing, employment decisions, and investment due diligence or other purposes, without consent, under the bill. Yet, while the HHS regulations under the Health Insurance Portability and Accountability Act (HIPAA) prohibit such uses for health insurers, this bill does not prohibit such uses for numerous other insurers or entities—such as auto, life, property and casualty and certain disability insurers.

Private Right of Action: Neither bill would amend Title V to grant consumers a private right of action for violations. Consumers deserve the right to enforce violations of their medical financial privacy.

Access: The bill establishes that consumers have access to their files and a right to correct errors. We would strongly recommend that instead of establishing such a narrow right that only applies to medical financial privacy, why not take the language of the administration bill and amend Title V to apply these stronger, important Fair Information Practice rights to all information held by financial services holding companies? This change would obviate one of the industry's running complaints about complexity of regulations. Instead of having strong access and correction provisions apply only to some information, make the law less complex and less burdensome by giving consumers these rights in all information covered under the Act, thereby establishing only one rule for firms to comply with, instead of two.

Stronger Law Controls: Both bills include language describing their relationship to HIPAA. Despite this provision, we believe that there may be overlaps and conflicts between the laws. We would suggest two changes. First, the inclusion of a more explicit section that clarifies that in all cases of overlap, the stronger, more pro-privacy protection applies. Second, we would

suggest that the notion of describing a relationship to "regulations," rather than statutes, may prove problematic and deserves clarification before markup. For example, what if the regulations are amended under a successor administration?

Conclusion:

We are pleased to support HR 4585 with the modifications above. It closes important loopholes in the Act and protects the most sensitive, unprotected information about consumers from misuse. If enacted, the bill would protect consumer medical financial privacy information through an opt-in, express consent system. We are encouraged that both the President and the Chairman of the committee have adopted the concept of opt-in consent and strong privacy protection that has been supported by a broad consensus of American privacy, civil liberties, consumer, and pro-family organizations[5] and championed by a growing, bi-partisan number of members. Now, we need to extend the Chairman's opt-in provision on medical information, and the President's opt-in provision on medical information and sensitive financial information, to all information held by entities under the Act.[6] We believe that the Chairman's bill offers an important template for extending this concept. We hope that the Chairman, Mr. LaFalce and the President will work together to expand the Chairman's bill before markup, so that the final bill addresses other major loopholes in the Act. Thank you for the opportunity to share our views.

ENDNOTES:

[1] U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups. PIRGs are non-profit, non-partisan consumer and environmental advocacy groups active around the country.

[2] For more details on PIRG's Financial Privacy Platform, see <http://www.pirg.org/consumer/banks/action/privacy.htm>

[3] As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html > The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 50-51.]

1.Collection limitation. There must be no personal data record keeping systems whose very existence is secret.

2.Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3.Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4.Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5.Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

[4] Of course, it is our view that HR 4380, which adopts a mixed opt-in/opt-out approach for financial privacy protection, should be strengthened to a full opt-in approach across the board, as HR 3320 (Markey) would provide.

[5] For a list of organizations that make up the informal Shelby-Markey Financial Privacy Coalition, see the letter 16 groups sent to financial regulators last month condemning the delayed implementation of Title V, the privacy provisions of the act, at http://www.consumer.org/consumer/glbdelay.htm

[6] And then, of course, to resolve the egregious gaps in U.S. privacy law by working to extend opt-in consent and other Fair Information Practices to all use of consumer information, whether financial, medical, Internet or otherwise.

GEORGETOWN UNIVERSITY

Georgetown Public Policy Institute

Testimony before the

U.S. House of Representatives

Committee on Banking and Financial Services

on

H.R. 4585
The Medical Financial Privacy Protection Act

Joy Pritts, Senior Counsel
Health Privacy Project
Institute for Health Care Research and Policy
Georgetown University

June 14, 2000

Mailing Address:
Institute for Health Care Research and Policy
2233 Wisconsin Avenue NW Suite 525
Washington DC 20007
202-687-0880 FAX: 202-687-3110

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the House Committee on Banking and Financial Services: I very much appreciate the invitation to testify before you today on H.R. 4585, a bill intended to amend the Gramm-Leach-Bliley Act (also known as the Financial Services and Modernization Act of 1999) in order to fill the health privacy gaps in the Act.

The Health Privacy Project was launched in December 1997 at the Institute for Health Care Research and Policy at Georgetown University. The Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. In the past year, the Project has published a number of resources on health privacy including *Best Principles for Health Privacy: A Report of the Health Privacy Working Group*; *The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes)*; and *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*. All of the reports are available on our Web site at http://www.healthprivacy.org. In addition, the Project coordinates the Consumer Coalition for Health Privacy, which is comprised of a broad cross-section of consumer and disability rights groups committed to educating and empowering healthcare consumers to have a more prominent voice on health privacy issues at the federal, state, and local levels.

At the outset, we would like to express our appreciation to Chairman Leach for his acknowledgment that there are significant health privacy gaps in the Gramm-Leach-Bliley Act (hereinafter "the Act"). We too believe that there are significant shortcomings in the Act.

The primary purpose of the Act was to enhance competition in the financial services industry by providing for the affiliation of banks, securities firms, insurance companies, and other providers of financial services. The idea is to offer "one stop shopping" for financial services. According to proponents of the Act, the exchange of personal data between affiliates is necessary to offer the kind of integrated financial services the bill is supposed to promote. But privacy advocates are concerned that allowing the exchange of this data, including medical or health information, endangers the privacy rights of consumers.

As enacted, however, the Act essentially allows the free-flow of a consumer's personal financial information among affiliates without the knowledge or authorization of the consumer. The Act only places restrictions on disclosures to "nonaffiliated" third parties, and those restrictions are *de minimus*. Even those restrictions can be circumvented through joint marketing agreements.

In our comments on the proposed regulations to the Act, we noted that these deficiencies would best be remedied through legislation. As such, we are pleased that the Chairman has introduced legislation, and has held this hearing today. We also want to acknowledge that there have been additional efforts recently to amend the Act including an Administration proposal introduced by members in both the House and Senate, and a separate bill introduced by Senator Shelby (R-AL).

Finally, we must highlight that the Department of Health and Human Services is due to issue final health privacy regulations this fall, as required by the 1996 Health Information Portability and Accountability Act of 1996. The proposed federal health privacy regulations constitute a significant step towards restoring the public trust and confidence in our nation's health care. These rules, however, are by no means the final solution. By virtue of the limited authority delegated by Congress, the proposed rules have limited applicability and cover only health plans, health care clearinghouses, and health care providers who transmit health information ("covered entities") in electronic form. As such, a large segment of those who hold health information remains beyond the scope of these regulations. Therefore, it is important that the Financial Services Act be amended to establish clear and enforceable privacy rules for those entities not covered by the HIPAA regulations.

Our testimony today focuses on the major provisions of H.R. 4585: restrictions on disclosure; limitations on use; voluntary consent; the right to see and correct health information; and the relationship to other laws. As background, we have included brief information about the need to protect the privacy of people's health information.

II. PUBLIC NEED AND DEMAND FOR HEALTH PRIVACY

The public has consistently expressed a high degree of concern over the vulnerability of their privacy, and the vulnerability of their health information in particular.

In the absence of meaningful and enforceable privacy protections, people are withdrawing from full participation in their own health care. People are afraid that their health records will fall into the wrong hands, and lead to discrimination, loss of benefits, stigma, and unwanted exposure. A January 1999 survey by the California Health Care Foundation found that one out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information, including lying to their doctors, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and — in the worst cases — avoiding care altogether.

Without trust that the personal, sensitive information they share with their doctors will be handled with some degree of confidentiality, people will not fully participate in their own health care. As a result, they risk inadequate care or undetected and untreated health conditions. In turn, the integrity of research and public health initiatives that rely on complete and accurate patient data may also be compromised. Thus, protecting privacy and promoting health care quality and access are values that must go hand-in-hand.

III. STRENGTHS AND WEAKNESSES OF H.R. 4585

If enacted, H.R. 4585 would take a large step forward in filling the privacy gaps in the protection of health information within the context of the financial services industry. However, we do have a number of concerns about the bill. Due to the limited time we have had to review this bill, we will focus our testimony today on some of the major provisions in H.R. 4585.

A. Increased Restrictions on Disclosure

One of the major weaknesses of the Gramm-Leach-Bliley Act is the minimal protections afforded by its restrictions on the sharing or disclosure of "nonpublic personal information." Under the Act, a financial institution can disclose nonpublic personal information, including individually identifiable health information, freely with its affiliates without any consent from the consumer. As for disclosures to nonaffiliates, the Act only requires notice of the potential disclosure and an opportunity for the consumer to "opt out" of such disclosures.

H.R. 4585 would improve these privacy protections in two major ways:

- First, the restrictions on disclosures would apply to both **affiliates** and **nonaffiliates.**

From a consumer's perspective it is the disclosure of information beyond the original record holder that triggers concern. It makes little difference to a consumer whether the recipient of that information is affiliated with the financial institution. Therefore, the approach taken in H.R. 4585 is preferable to the requirements that currently exist in the Act.

- Second, under H.R. 4585 a consumer must affirmatively consent (**opt in**) to the disclosure of individually identifiable health information.

This approach parallels that taken in many other areas of Federal privacy law, where "opt in" is the norm. For example, a consumer "opt in" is required before a tax preparer could transfer information from a consumer's tax return to a financial advisory affiliate to provide the consumer with financial planning advice. An "opt in" is required before a video rental store can provide information regarding a consumer's videocassette rentals to others. "Opt in" is required before telephone companies can transfer information about what telephone numbers a consumer calls or the whereabouts of the cellular phone the consumer is using to other parties. "Opt in" is required before cable television companies can provide information about what pay-per-view movies a consumer is watching to other parties.

We commend the adoption of an opt in requirement for the disclosure of individually identifiable health information within the financial services context. However, it is critical that this opt in be voluntary and uncoerced. (See "C" below.)

B. Limitations on the Use of Individually Identifiable Health Information

One of the major concerns of health consumers is that they might be injured economically by a financial institution's use of their health information. The Act does not address this concern. H.R. 4585 moves towards correcting this problem by prohibiting financial institutions from obtaining or using individually identifiable health information in deciding whether to issue or continue credit or loans absent the consumer's affirmative consent. We support the general concept behind this provision which appears to alleviate one of the strongest concerns of consumers–that they might be denied a loan or a mortgage due to a health condition.

We are concerned, however, that this protection is limited only to uses for purposes of providing a "loan or credit" and does not apply more broadly to "financial transactions" in general. The current language would allow uses of health information obtained without a consumer's consent for *any* insurance transaction and for any other financial transaction that is not the provision of a loan or credit. We recognize that *some* insurance transactions (which would fall in the general category of "financial transactions") would require the disclosure of health information. We believe, however, that these interests could be served by obtaining the consent of the consumer.

We appreciate the fact that H.R. 4585 attempts to limit the circumstances under which a financial institution can *request* a consumer's consent to receive health information. The terms of the limitation, however, are somewhat confusing.

C. Voluntary Consent

We urge that H.R. 4585 be amended to include a provision ensuring that the opt in privacy protection is truly voluntary and meaningful. We recommend the adoption of provisions that would prohibit financial institutions from conditioning the delivery of a financial service or product on the consumer's signing an authorization allowing the financial institution to receive their health information. An authorization requirement is not very meaningful if the consumer can be coerced into providing such a requirement as a condition of receiving a benefit or service. We recognize that there are some legitimate circumstances for requiring an authorization for the receipt of health information as a condition to providing some financial services (such as some types of insurance transactions) but these should be the *exception* and not the rule.

D. Right to See and Correct Health Information

H.R. 4585 grants consumers the right to access and correct their individually identifiable health information that is within the possession of the financial institution. We strongly support the general concept behind this amendment to the Act. Financial institutions may base important decisions on an individual's health information. It is important that the consumer be able to

verify that this information is accurate and, if necessary, to correct inaccurate information. We believe, however, that the right of access granted is too narrow. The right of access should not be limited to health information that is "within the possession" of the financial institution but should include information that is within the institution's *control.*

E. Relationship to Other Laws

As noted above, the Department of Health and Human Services is in the process of promulgating privacy standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA privacy standards will apply to many of the same insurers that are subject to the Gramm-Leach-Bliley Act. We are pleased that H.R. 4585 expressly provides that it does not modify, limit or supersede the privacy standards being promulgated by HHS. It appears that this provision, in conjunction with other language in the Gramm-Leach-Bliley Act, will leave stronger state privacy laws intact. As detailed in our report, *The State of Health Privacy: an Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes* (July 1999) many states have detailed laws governing the use and disclosure of individually identifiable health information by insurers. The state protections which are stronger should stand.

IV. CONCLUSION

While there were unsuccessful attempts to remedy these privacy problems before final passage of the act last summer, we are heartened by your efforts to finish the job this year. We are available to work with you and the staff of the committee in moving this critical provision forward. H.R. 4585 is an essential piece of the overall effort to ensure that Americans have basic health privacy protections. Through the passage of this bill, the final regulations issued by the Secretary, and other health privacy legislation being considered by the Congress, we can help to meet this goal.

Testimony of

RONALD WEICH

Partner - Zuckerman, Spaeder, Goldstein, Taylor & Kolker, L.L.P.
Legislative Consultant to the American Civil Liberties Union

ON BEHALF OF
THE AMERICAN CIVIL LIBERTIES UNION

Before the
House Committee on Banking and Financial Services

on

"H.R. 4585 – the Medical Financial Privacy Protection Act"

June 14, 2000

Mr. Chairman and Members of the Committee: My name is Ronald Weich. I am a partner in the law firm of Zuckerman, Spaeder, Goldstein, Taylor & Kolker, and a legislative consultant to the American Civil Liberties Union (ACLU). I am pleased to appear before you today on behalf of the ACLU to discuss the issue of medical privacy in the financial services industry, and to provide our views on the Medical Financial Privacy Protection Act (H.R. 4585) proposed by Chairman Leach.

The ACLU is a nationwide, non-partisan organization of nearly 300,000 members dedicated to protecting the principles of liberty, freedom and equality set forth in the Bill of Rights to the United States Constitution. For almost 80 years, the ACLU has sought to preserve and strengthen privacy in all aspects of American life.

My testimony is divided into two parts. The first section presents an overview of the need for medical privacy protections in federal law. The second section discusses the civil liberties implications of the Chairman's proposal to address medical privacy in the financial industry.

I. The Importance of Medical Privacy

Advances in technology have brought about a revolution in every aspect of health care, including the manner in which medical information is maintained and disseminated. Today, medical data can be collected, combined, collated, analyzed and distributed faster and easier than ever before. Huge quantities of health-related information can be stored electronically and transmitted across the country and around the globe with the click of a computer mouse.

Much of this electronic activity benefits individual patients and facilitates public health efforts as well. But, like many technological advances, society's increased reliance on computerized medical records presents significant challenges to privacy. In the absence of legal safeguards, computerization allows for virtually unlimited access to medical records without the knowledge or consent of the patient whose records are accessed.

Privacy is vital in the health care context because trust is a fundamental component of the doctor-patient relationship. Since medical records contain particularly sensitive and intimate information, patients are susceptible to humiliation and discrimination in the event information from their medical records is improperly disclosed. If patients are not confident that their medical privacy will be respected, they will be less likely to seek medical care, and less willing to be candid with medical professionals about their health. The fear of losing medical privacy, therefore, may lead to adverse health consequences for individuals. The failure of individuals to seek medical treatment may also lead to dangerous public health conditions, for example in the areas of sexually transmitted diseases and substance abuse.

At the same time that computer technology has made medical record keeping vastly more efficient and therefore less reliably private, the confidentiality of medical records is separately threatened by the trend toward economic integration of financial institutions, some of which have access to their consumers' personal medical information. Last year Congress enacted a financial services modernization law, now known as the Gramm-Leach-Bliley Act, that dramatically facilitates the merger of – and therefore the sharing of information between -- banks, insurance companies and other financial entities.

The ACLU regrets that the financial services modernization law did not include stronger privacy protections in general. But we are especially concerned that the bill lacks medical privacy protections, since medical information is among the most sensitive categories of information that integrated financial entities will now be able to share with each other. While we recognize that some commercial uses of personal medical information are legitimate and beneficial to consumers, we believe that other commercial uses of medical information are illegitimate and invasive of personal privacy.

The task for Congress now is to sort out the permissible and impermissible uses of medical information in the financial services sector, and to establish a process by which consumers can participate meaningfully in decisions about their own medical information.

It is fair to ask why consumers have any role at all in this process, if the records in question are generated and maintained by commercial entities rather than individual patients. The answer, in our view, is that patients own their medical records, and that health care providers or insurance companies who maintain those records should be viewed as custodians of the patients' property. We believe that medical records in the possession of health care professionals or third party payors are like client files in the possession of attorneys. The patient or the client retains ultimate control over the disclosure of information in their records. If follows that (1) patients may reasonably expect that their personally identifiable health information will not be disclosed to anyone unless they have given specific and express written consent, and (2) medical records must be protected from unauthorized access to the fullest extent practicable.

These straightforward objectives are elusive because the United States lacks a coherent and consistent medical privacy policy. A patchwork of state laws affords varying levels of protection to citizens in some jurisdictions. That is insufficient. The ACLU continues to urge Congress to enact an omnibus medical privacy law that would provide a consistent and reliable set of privacy protections for medical records in all settings, including the financial services industry.

In the absence of such a law, we have supported the current regulatory process in which the Department of Health and Human Services is finalizing rules to implement medical privacy directives contained in the 1996 Health Insurance Portability and Accountability Act. The ACLU has submitted detailed comments to HHS urging that these regulations be strengthened in key respects.

It is important that less comprehensive congressional efforts to protect medical privacy, such as this Committee's consideration of privacy protections in the financial services industry, not hinder the broader efforts to enact a medical privacy policy through statute or regulation. During consideration of the Gramm-Leach-Bliley legislation last fall, we urged rejection of the so-called Ganske amendment that we believe could have undermined the HHS regulatory process. We appreciated the willingness of this Committee to consider our views and to remove the amendment in conference. We also appreciate the Chairman's recognition that this is now an issue that Congress must address.

With these considerations in mind, I will now turn to specific comments about the bill before the Committee today, H.R. 4585.

II. Civil Liberties Implications of H.R. 4585

We commend Chairman Leach for introducing a bill designed to address the significant deficiencies of the Gramm-Leach-Bliley law in the area of medical privacy. At the time Gramm-Leach-Bliley was considered, some argued that the generic privacy protections in the bill were sufficient to meet concerns about the transfer of sensitive medical information among financial affiliates. The ACLU disputed that assertion, and we view the introduction of H.R. 4585 and this hearing as a welcome acknowledgment that medical records deserve heightened protection in the financial world.

Indeed, we hope that the introduction of H.R. 4585 signals a willingness by Congress to reconsider the broader decisions it made about financial privacy in the Gramm-Leach-Bliley Act.

In general, the ACLU supports an "opt-in" privacy model under which individually identifiable health information may not be disclosed among component entities of a financial institution unless the institution provides notice to the subject of the information and obtains verifiable consent prior to disclosure. While we are pleased that H.R. 4585 generally adopts this approach, we believe there are certain ambiguities in the proposal that should be clarified and other improvements that should be made during this Committee's consideration of the bill.

A threshold question is the relationship between this bill and the forthcoming HHS regulations. Proposed section 502A(e) provides that nothing in the new law would "modify, limit or supercede" standards promulgated by the Secretary of Health and Human Services. That is generally the right approach, although there may be instances in

which this bill provides even stronger privacy protections than the regulations, and when that occurs we believe this law should govern. Whenever there is a conflict between the regulation and the law, the rule that provides greater privacy protection for consumers should prevail.

Let me now suggest several specific ways in which the protections in H.R. 4585 could be strengthened.

A. Right to Withdraw Consent

H.R. 4585 requires that before individually identifiable health information is disclosed by a financial institution, the individual who is the subject to the information must be given written notice of the disclosure and the financial institution must elicit the affirmative consent of the individual prior to disclosure of records. This approach embraces the fundamental principle that individuals should control the use of their medical records. But this principle also dictates that a consumer should be able to withdraw his or her consent for the use of health information.

Proposed section 502A(a)(1)(B) is ambiguous on this point. It provides that "[a]ny withdrawal of consent is subject to the rights of any financial institution that acted in reliance on the consent prior to its withdrawal." The bill does not explain what the rights of financial institutions are in this regard, but we fear that the allusion to such rights could serve to blunt what should be the absolute right of a consumer to withdraw consent. This is especially important in a context where consent will sometimes be granted at the outset of a relationship between the consumer and a financial institution, and the consumer will subsequently learn of practices that he or she regards as a breach of privacy.

We urge that section 502A(a)(1)(B) be deleted. If a financial institution has, in fact, detrimentally relied on a consumer's prior consent, standard contract law principles may provide legal rights that will govern the transaction whether or not referenced in statute. This ambiguous provision can only diminish the rights of consumers and undermine the general principle that withdrawal is be effective upon receipt by the financial institution.

B. Right to Access and Correct Records

The bill appropriately includes a mechanism (proposed section 502A(c)) for accessing and correcting individually identifiable health information contained in the records of financial institutions. Damaging inferences may be drawn about an individual from incorrect health information. The opportunity to prevent or minimize the harm caused by inaccurate data entries or other incorrect information is fundamental to ensuring that individuals are treated fairly by those who view their records. Accordingly, the process for correcting records is critical to the protection of the interests at stake in this bill.

To this end, proposed section 502A(c)(1)(A) should be strengthened to require a financial institution to provide customers with access to information that is "under the control of the financial institution," not just information that is "within the possession of the financial institution." This modest change prevents financial institutions from avoiding the responsibility imposed by this provision simply by transferring its information to an affiliated entity.

C. Exceptions to Non-Disclosure

A significant flaw in H.R. 4585 is the broad scope of the exceptions it permits to the general rule of nondisclosure. Certain exceptions which facilitate transactions or which pertain to other routine business functions of financial institutions may be warranted. But the bill carves out broad exceptions in other areas that severely undermine the protections afforded under the general provisions of H.R. 4585.

First, it is difficult to imagine how a financial institution could protect the confidentiality or security of its records pertaining to a customer by disclosing nonpublic personal information about the customer as permitted under section 502(e)(3)(A) of the Gramm-Leach-Bliley Act. We urge that this exception to the general non-disclosure rule should be eliminated.

Second, the exceptions for persons "holding a legal or beneficial interest relating to the customer," or "acting in a fiduciary or representative capacity on behalf of the customer" as provided in section 502(e)(3)(D) and (E) of the Gramm-Leach-Bliley Act unjustifiably limit the privacy rights of minors, particularly with respect to their reproductive health care. The proposed HHS rules carefully address this issue, and should not be undercut by more generic language in this bill.

Third, the exception for requests made by law enforcement and governmental agencies is overly broad to the extent that it expands on the investigative exceptions set forth in the Right to Financial Privacy Act of 1978, 12 U.S.C. §3401 et seq. and other existing laws pertaining to the investigation of financial institutions. Any "investigation on a matter related to public safety" should be conducted in accordance with the

provisions of the Right to Financial Privacy Act. The provisions of that law are already contemplate such investigations and any governmental unit conducting such an inquiry should be compelled to comply with the notice provisions in the 1978 Act. Therefore, section 502(e)(5) of the Gramm-Leach-Bliley Act should be modified to clarify that no expansion of existing law enforcement authority is intended.

Fourth, there is no basis for a financial institution to disclose individually identifiable health information about its customers to "self-regulatory organizations." Whatever the administrative functions of such organizations, they should be carried out using aggregate or de-identified information. Therefore this exception in section 502(e)(5) of the Gramm-Leach-Bliley Act should not be applicable to individually identifiable health information.

Finally, section 502(e)(8) of the Gramm-Leach-Bliley Act duplicates the exceptions set forth in section 502(e)(5). We propose that for clarity's sake, the provision should be modified to reflect that this exception pertains only to judicial proceedings involving or action taken by governmental regulatory authorities with jurisdiction over the financial institution. Any law enforcement or other government agency seeking individually identifiable health information about a particular person must comply with the Right to Financial Privacy Act of 1978.

D. Mental Health Protections

The enhanced protections for mental health records in H.R. 4585 is commendable, but should also be afforded to information about other sensitive records such as those pertaining to reproductive health, sexually transmitted diseases and substance abuse

treatment. Just as financial institutions should be required to obtain a consumer's separate and specific consent with respect to the disclosure of, for example, psychotherapy records, so should such specific consent be required for equally sensitive health records.

E. Private Right of Action.

H.R. 4585 fails to provide consumers with a meaningful remedy in the event their individually identifiable health information is improperly disclosed. Regulatory oversight of financial institutions is an insufficient means of policing the vast financial services industry. The absence of a private right of action is, of course, one of the limitations of the HHS medical privacy regulations as well. Congress should establish a mechanism for individuals to receive compensation for wrongful disclosure of their identifiable health information in order to deter this conduct.

F. Genetic Privacy

While H.R. 4585 creates an opportunity for consumers to consent to the disclosure of their health information to financial entities, it does not fully address circumstances in which disclosure of health information should not be permitted because the information should never be used for commercial purposes. The primary example of that concern is the potential disclosure to insurers and others of genetic information about individual consumers.

Scientists will soon complete a map of the entire sequence of human genes. While this breakthrough holds great promise for improving medical treatments, it also presents unique challenges to principles of privacy and non-discrimination. The ACLU believes

that genetic information should not be a basis to discriminate against individuals in employment or insurance, for three reasons:

First, it is inherently unfair to discriminate against someone because of immutable characteristics that do not limit their abilities.

Second, the mere fact that someone has a genetic predisposition to a health condition is an unreliable basis to act on the assumption that he or she will actually develop that condition in the future. Genetic tests do not show with certainty that any individual will eventually develop the disease or how severe their symptoms might be.

Third, the threat of genetic discrimination in insurance or employment may lead individuals to decline genetic screenings and other health services to avoid bringing to light information that may be used against them. For example, the Journal of the American Medical Association reports that only 57% of women at risk for breast cancer seek genetic testing, and 84% of those who decline the test do so because they fear genetic discrimination.

Congress has before it legislation to protect all Americans against discrimination based on their genetic information. Senator Daschle and Congresswoman Slaughter have each introduced legislation (S. 1322; H.R. 2457) that would provide comprehensive protections against genetic discrimination. The ACLU supports these proposals, and urges that they be incorporated to the maximum extent feasible in H.R. 4585.

It is especially important to ban databases containing personally identifiable genetic information. Once genetic information is in the hands of an insurer or employer,

there are corporate pressures to use it. Prohibiting the compilation of personally identifiable genetic data would minimize this risk.

CONCLUSION

The American Civil Liberties Union appreciates the opportunity to present its views on this important subject and would welcome the opportunity to work with this Committee as it continues its consideration of H.R. 4585 and other medical financial privacy proposals.

Statement

of

America's Community Bankers

on

H.R. 4585, the "Medical Financial Privacy Protection Act"

before the

Committee on Banking and Financial Services

of the

U.S. House of Representatives

on

June 14, 2000

[Submitted for the Record]

America's Community Bankers is pleased to submit testimony for today's hearing before the House Banking and Financial Services Committee on medical information privacy. ACB represents the nation's community banks of all charter types and sizes. Our members pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

Mr. Chairman, ACB commends you for holding this hearing on medical information privacy and your legislation, H.R. 4585, the "Medical Financial Privacy Protection Act." Given its unique sensitivity among the general public, the treatment of private medical information is an issue which deserves close examination by Congress in a public forum, such as today's hearing.

Community banks are well aware of the importance of protecting the confidentiality of customer information. Community banks across the country are in the midst of complying with the requirements of the most sweeping law in American history to protect the financial information privacy interests of consumers. The implementation of the privacy provisions of the Gramm-Leach-Bliley Act (GLBA) will ensure consumers of financial services that their personal information will continue to be safeguarded by their local community bank and other financial institutions.

One area of customer information privacy that was not directly addressed by the GLBA was the confidentiality of medical information. Congress chose this approach, despite the best efforts of you, Mr. Chairman, to include in the GLBA an opt-in requirement for the disclosure of individually identifiable health and medical information. ACB strongly supported this initiative. Instead, Congress made the decision to wait until the U.S. Department of Health and Human Services (HHS) could develop federal standards governing the treatment of such information under the authority of the "Health Insurance Portability and Accountability Act of 1996."

ACB continues to support public policy that lenders receive the affirmative consent of a consumer before that consumer's individually identifiable health information can be disclosed to another party.

Frankly, the vast majority of our members do not have access to individually identifiable health information, nor do they seek to obtain such information in making decisions to offer loans or extend credit.

While ACB stands behind this public position on medical information privacy, we do encourage Congress to refrain from passing additional legislation before all currently authorized regulatory remedies, such as the regulations being developed by the HHS, are exhausted. Legislative efforts to reopen the GLBA, no matter how targeted, could result in new, harmful restrictions on the ability of community banks and other financial institutions to legitimately use information. We do, however, commend Congressional efforts, such as today's hearing, to publicly examine such issues of public concern.

○